Haaga-Helia
ammattikorkeakoulu Oy

Microsoft Active Directory palvelimen tietoturvan parantaminen

Joni Hakala

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2021

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä
Joni Hakala

Koulutusohjelma
Tietojenkäsittelyn koulutus, tradenomi (AMK)

Raportin/Opinnäytetyön nimi
Microsoft Active Directory palvelimen tietoturvan parantaminen

Sivu- ja liitesivumäärä
35 + 2

Tutkimuksen tarkoitus on parantaa Microsoft Windows Active Directory palvelimien tietoturvaa, koska yleisin käyttötarkoitus Windows palvelimelle on asentaa Active Directory organisaation keskitetyn hallinnan työkaluksi. Tutkielman tietoperusta koostuu aktiivisen puolustamisen malleista OODA-silmukka, CIA-kolmio, riskienhallinta ja parhaat käytännöt. Tutkimusmenetelmässä tutkitaan aktiivisen puolustuksen ja parhaiden käytäntöjen merkitystä hyökkäävästä näkökulmasta Intrusion Kill Chain menetelmän avulla, demonstroimalla oikeita hyökkäyksiä.

Tutkimus koostuu neljästä vaiheesta. Ensimmäisessä vaiheessa selvitetään, aktiivihakemiston tietoturvan tärkeys ja tärkeitä toimintoja. Tutkielman toisessa vaiheessa selvitetään aktiivisen puolustuksen menetelmiä, loppukäyttäjän vastuut ja parhaita käytäntöjä aktiivihakemisto palvelimelle. Kolmas osa koostuu mahdollisten hyökkäystyyppien ja hyökkäysvektoreiden kartoittamisesta. Tutkimuksen neljäs osa eli tutkimusmenetelmän tarkoituksena tutkia erilaisia hyökkäystapoja, että saadaan parempi kuva siitä mitä tapahtuu, jos ei noudata parhaita käytäntöjä ja aktiivisen puolustuksen menetelmiä. Tutkimusmenetelmänä testaus ja havainnollistaminen, koska hyökkäyksiä on vaikea estää, jos ei edes tiedetä minkä kaltaisia hyökkäyksiä järjestelmää vastaan voidaan oikeasti toteuttaa. Tutkimusmenetelmän idea on lähtöisin muista tutkielmista, joissa kehotetaan käyttämään aktiivisen puolustuksen menetelmiä ja parhaita käytäntöjä, mutta eivät kerrota tai näytetä esimerkkejä mitä voi tapahtua, kun niitä ei noudateta.

Tutkielman kaikki eri vaiheet tukevat pääaihetta, joka on aktiivihakemiston tietoturvan parantaminen. Myös hyökkäysvaiheen tarkoituksena on aktiivihakemiston tietoturvan parantaminen, sillä järjestelmän puolustuksessa tulee ottaa huomioon myös mahdolliset hyökkäystavat ja miten hyökkääjät ajattelevat.

Asiasanat
Active Directory, kyberturvallisuus, tietomurto, tietoturva, turvatoimet, Windows Server

Sisällys

1 Johdanto

Opinnäytetyön tarkoituksena tutkia Microsoft Active Directory palvelimen tietoturvaan tutkielmana puolustavasta ja hyökkäävästä näkökulmasta. Tutkielmassa tutustutaan Windows palvelimien parhaisiin käytäntöihin ja tietoturvaan. Tietoturvaa tutkitaan suosittujen tietoturvamenetelmien kautta aktiivisella puolustuksella ja soveltamalla erilaisia oikeita hyökkäystapoja palvelinta vastaan käytännössä. Tutkielma vertaa hyökkäyksiä tieteis- lähteiden suosittelemiin parhaisiin käytäntöihin, menetelmiin ja asetuksiin. Hyökkäyksien avulla saadaan realistinen kuva palvelimen tietoturvasta ja huonoista käytännöistä Windows palvelimen tietoturvaan katsottuna. Oppimistavoitteena on opetella tietoturvan menetelmiä Windows ja Linux käyttöjärjestelmillä. Opinnäytetyön tavoiteltu hyöty parantaa Active Directory palvelimen tietoturvaa ulkoisilta hyökkääjiltä aktiivisen puolustuksen menetelmillä ja havainnollistamalla miten oikeat hyökkäykset voivat toimia käytännössä. Hyökkäyksien avulla lukija saa hyvän kuvan, miten tietoturvan menetelmät toimivat, miten ulkopuoliset hyökkäykset toimivat käytännössä ja miten palvelin pidetään turvallisena. Tuloksena projektista syntyy opinnäytetyö tutkielma Windows palvelimen yleisestä tietoturvasta. Tuloksia voi hyödyntää Windows palvelimia käyttävät tahot tietoturvan parantamisessa.

Tutkimuksessa ei käsitellä todella vanhoja tietoturva aukkoja vaan keskitytään Microsoftin uuteen Windows 2019 palvelimeen, jossa on asennettuna Active Directory. Tietoturvaa tarkastellaan sillä oletuksella, että fyysinen tietoturva on kunnossa eli palvelin on turvallisesti lukitussa tilassa ja siihen ei pääse käsiksi. Tutkielmaa ei rajata pelkästään Active Directoryn tietoturvaan vaan kaikkiin Windows 2019 palvelimista löytyviin tietoturva aukkoihin, koska ne voivat olla jalansija Active Directoryn tietoihin. Tutkielmassa käytetään menetelminä tieteis- kirjoituksien tulkinta, aktiivinen puolustus, hyökkäysmenetelmien kokeilu, kohteen tiedustelu ja kohteeseen murtautuminen. Kokeiluvaiheessa hyökkäävänä käyttöjärjestelmänä käytetään Kali Linuxia ja hyökkäyksen pääkohteena Windows Server 2019 palvelinta.

Tutkimusmenetelmän tarkoituksena kartoittaa tietoturva ongelmia kokeilemalla miten parhaat käytännöt voidaan tehdä väärin ja miten voidaan murtautua väärin konfiguroituun Active Directory palvelimeen. Tutkielman tarkoituksena parantaa Active Directory palvelimen tietoturvaa tutkimalla suositeltuja parhaita käytäntöjä, aktiivista puolustamista ja hyökkäämisen menetelmiä. Tutkimuksen aiheideana yhdistää puolustavat tietoturvan käytännöt, hyökkäyksien havainnollistamiseen eli oikean hyökkäys tilanteen kokeiluun. Tutkimuksessa katselmoidaan parhaiden käytäntöjen, aktiivisen puolustamisen ja hyökkäyksen suhdetta toisiinsa. Tutkimus on vaan yksi näkökulma aiheeseen eikä käy kaikkia mahdollisia puolustus tai hyökkäys tilanteita läpi.

Tutkimuksen tavoitteena parantaa Active Directoryn tietoturvallisuutta tunnettujen tietoturvamenetelmien avulla. Tutkimuksen prosessin ensimmäinen vaihe tutkia miksi Active Directoryn tietoturva on tärkeä aihe. Seuraavaksi tutkitaan Active Directoryn parhaita tietoturvakäytäntöjä ja asetuksia tietoturvan parantamiseksi. Tutkielman keskivaiheessa käydään läpi aktiivisen puolustamisen taktiikoita ja yleisiä hyökkäystapoja. Tutkielman loppuvaiheilla tutkitaan oikeiden hyökkäyksien toimintasuunnitelmia ja kokeillaan oikeita hyökkäyksiä. Hyökkäysvaiheen tarkoituksena vertailla tuloksia tutkielman tietoturvan parhaisiin käytäntöihin ja aktiiviseen puolustamiseen. Lopuksi tutkielmassa tarkastellaan tuloksia ja pohditaan kokonaisuutta.

Tämä opinnäytetyö ei ole absoluuttisen tietoturvan takaava tutkielma, koska täysin turvallista verkkoa, järjestelmää, laitteistoa tai ohjelmistoa ei ole olemassa. Lukijalle jää oma vastuu arvioida riskit omissa erityisolosuhteissa. Tutkielmassa käytetään oikeita hyökkäyksiä koulutustarkoituksessa, jotka ovat laittomia väärinkäytettyinä. Hyökkäys menetelmiä saa käyttää vain sallittuihin kohteisiin, joihin olet saanut kirjallisen luvan tehdä tunkeutumistestausta.

Tutkimuksen tarkoituksena selvittää kolmeen tutkimuskysymykseen vastauksia:

1. Miksi Active Directoryn tietoturva on tärkeää?
2. Mitä ovat Windows palvelimien parhaat käytännöt?
3. Miten parantaa Windows palvelimen tietoturvaa?

1.1 Ammattisanasto

Active Directory	Microsoftin kehittämä ohjelmisto organisaatioiden tietojärjestelmän resurssien keskitettyyn hallintaan.
Administrator	Järjestelmänvalvojan käyttäjätunnus, jolla suoritetaan toimintoja, jotka edellyttävät erityiskäyttöoikeuksia.
Apache2	Ohjelmisto, jolla voidaan isännöidä verkkosovelluksia palvelimelta.
C2	Lyhenne (Command & Control) tai suomeksi komenna ja hallitse yleisesti katastrofitilanteissa käytetty viestintäjärjestelmä.
CIA-kolmio	Lyhenne (confidentiality, integrity, ja availability kolmio) on menetelmä, jolla ohjataan tiedon säilytyksen parhaita käytäntöjä.
CVSS	Lyhenne (Common Vulnerability Scoring) on standardoitu menetelmä arvioida tietoturva haavoittuvuuksien vakavuutta.

DCSync	Hyökkäysmenetelmä verkkotunnus ohjain järjestelmäkäyttäjää vastaan, joka hakee käyttäjien tunnistetietoja.
DLL-tiedosto	Lyhenne (Dynamic-link library) on Microsoft käyttöjärjestelmissä dynaamisten linkkien kirjastotiedosto.
Verkko nimipalvelin	Palvelin, joka muuntaa IP-osoitteet verkkonimi osoitteeksi loppukäyttäjille.
Verkkosovellus	Palvelu, jota isännöidään verkkoon ja on yleisesti avattavissa verkkoselaimella.
Verkkotunnus	Organisaation rekisteröimä verkkotunnus, jonka avulla käyttäjä löytää palvelun ilman IP-osoitetta.
Eettinen hakkeri	Tietoturvan asiantuntija, jonka yritys on palkannut tekemään tunkeutumistestausta palvelimelle.
EvilWinRm	Hyökkäys ohjelmisto, jolla saadaan terminaali etäyhteys Windows palvelimille.
ICT	Lyhenne (Information and communications technology) tai suomeksi tieto- ja viestintätekniikka, jota käytetään laajana terminä tietotekniikalle.
Impacket	Kokoelma kirjasto Python skriptejä, joita hyökkääjä voi hyödyntää palvelimeen tunkeutumisessa.
Intrusion Kill Chain	Tunkeutumisen tappoketju on menetelmä, jota käytetään palvelimen puolustamisessa tai palvelimeen hyökkäämisessä.
IP-osoite	Verkko osoitteiden protokolla tarvitaan jokaiselle laitteelle, joka käyttää internet-protokolla viestintää.
IT	Lyhenne (Information technology), joka tarkoittaa tieto- ja viestintätekniikka alan osa alueita.
NetLogon	Windows palvelimen todennusmekanismi, jota käytetään käyttäjien todennuksessa.
On-Demand	Palvelu, jota käytetään vain tarpeen vaatiessa.

OODA silmukka	Lyhenne (observe, orient, decide ja act silmukka) on menetelmä, joka on tarkoitettu päätöksien tekemisen tehostamiseen.
Pass-to-Hash	Hyökkäysmenetelmä, jossa hyökkääjä todentaa kirjautumisen palvelimelle salatulla salasanalla.
Palvelin	Muille laitteille, ohjelmistoille ja käyttäjille toimintoja isännöivä tietokone.
PHP	Ohjelmointikieli, joka soveltuu erityisesti verkkosovelluksiin.
Porttiskannaus	Sovellus, jonka tarkoituksena on tunnistaa palvelimen avoimet portit ja niistä vastaavat ohjelmistot.
Python	Ohjelmointikieli, joka on yleiskäyttöinen ohjelmointikieli.
Sanakirjahyökkäys	Hyökkäys tekniikka, joka hyödyntää sanalistaa arvaamaan tietty sana.
Sisäverkon osoite	Organisaation sisäisessä verkossa oleva osoite, joka ei näy julkiseen verkkoon.
Terminal	Tekstipääte, johon syötetään komentoja tietokoneen suoritettavaksi.
Tunkeutumistestaus	Tietoturvan tarkastusmenetelmä, jossa luvan saanut hyökkääjä suorittaa järjestelmän turvallisuuden tarkastusta hyökkäyksien avulla.
Zero Trust	Tietoturvan menetelmä, jossa käsitellään kaikki verkkoliikenne ikään kuin sen alkuperä olisi ulkoverkosta.
Zerologon	Kriittinen haavoittuvuus Microsoftin todennusprotokollassa, jota voidaan hyödyntää nollaamaan verkkotunnus ohjain järjestelmäkäyttäjän salasana.

2 Microsoft Active Directory

Active Directory eli aktiivihakemisto on Microsoftin kehittämä verkkotunnuksien käyttäjätietokanta ja hakemistopalvelu. Aktiivihakemisto on asennettavissa Microsoftin Windows palvelin käyttöjärjestelmissä ja on keskeinen osa organisaation tietoturvallisessa resurssienhallinnassa. Aktiivihakemistosta löytyy tiedot käyttäjätunnuksista, tietokoneista ja verkkoresursseista. Aktiivihakemisto mahdollistaa resurssien keskitetyn hallinnan käyttöoikeuksille, käyttäjille, tietokoneille, ryhmille, dokumenteille ja sovelluksille. Aktiivihakemiston tarkoitus on jakaa resurssit vain oikeutettujen käyttäjien käyttöön. Aktiivihakemistossa voidaan myös luoda ryhmäkäytäntöjä ryhmille, antaa oikeuksia resursseihin ja organisaation tietokoneet saa oikeudet tehdä toimintoja. (Microsoft 2017).

Kuva 1: Aktiivihakemisto

Aktiivihakemisto palvelimelle asentuu automaattisesti Domain Name Server eli verkkotunnuksien nimipalvelin, joka muuntaa IP-osoitteet verkkotunnus nimiin ja takaisin IP-osoitteisiin. Käyttäjät hyödyntävät verkkotunnuksien nimipalvelinta palvelimien löytämiseen ilman IP-osoitetta. Aktiivihakemisto käyttää verkkonimi palvelua tärkeimmissä toiminnoissa, kuten käyttäjät todennuksessa ja tietokoneet löytääkseen aktiivihakemisto palvelimen. Verkkonimi palvelu sisältyy kaikkiin Windows käyttöjärjestelmiin. Oletusarvoinen verkkonimi palvelu toimii asennuksen jälkeen toimivan verkkoyhteyden avulla. Verkkonimi palvelu toimii siis yhtenä lisäosana myös aktiivihakemistossa. (Ross, McIllece & Gerend 2020).

Aktiivihakemiston päätarkoituksena on hoitaa verkon sisäistä tunnistautumista ja sallia vain todennetut käyttäjät sisäverkon resursseihin. Sallimalla vain tunnistetut käyttäjät verkon sisällä organisaation sisäinen verkko pysyy turvallisempana. Aktiivihakemiston isoin hyöty on käyttäjien ja ryhmien keskitettyhallinta. Ilman aktiivihakemistoa jokaiselle organisaation koneelle pitäisi tehdä paikallinen käyttäjä ja salasanaa vaihdettaessa salasana pitäisi vaihtaa jokaiselle organisaation tietokoneelle yksittäin. Aktiivihakemisto mahdollistaa myös käyttäjäryhmille käytäntöjen luonnin ja hallinnan, jonka avulla kokonaiselle ryhmälle voidaan ottaa resursseja käyttöön. (Microsoft 2009).

2.1 Aktiivihakemiston tietoturvan tärkeys

Aktiivihakemisto ohjaa kokonaisen organisaation käyttäjien oikeuksia ja tietokoneita. Aktiivihakemistossa säilytetään kaikkien organisaation käyttäjien salasanat ja yleisesti myös arkaluonteisia dokumentteja organisaation jaetuissa verkkokansioissa. Aktiivihakemisto on siis yksi yrityksen tietoturvan kannalta tärkeimmistä palveluista ja syytä pitää tietoturvallisena. Aktiivihakemisto palvelin on hyökkääjälle todella tärkeä kohde, koska se mahdollistaa tehokkaan kiristyshaittaohjelman levityksen kaikkialle organisaation verkkoympäristössä (Kyberturvallisuuskeskus 2020.) Suurin osa isoista yrityksistä hyödyntää aktiivihakemistoa, Frost & Sullivan keräämän tiedon mukaan noin 90 % fortune 1000 yrityksistä hyödyntää Microsoftin aktiivihakemistoa käyttäjien todennuksessa. Aktiivihakemistolla voidaan parantaa yrityksen tietoturvaa, mutta väärin konfiguroituna ja ilman käyttäjäkoulutusta aktiivihakemistosta voidaan tehdä tietoturvaton. (Krishnamoorthi & Carleton 2020).

Aktiivihakemiston pakollisena lisäosana toimii verkkotunnuksien nimipalvelu, ohjaamaan käyttäjien autentikointia. Verkkotunnus nimipalvelu luotettavuus ja yksinkertaisuus voi luoda organisaation tietoturvalle sokea pisteen verkkotunnus nimipalvelusta. Jos verkkotunnus nimipalvelua ei pidetä turvallisena hyökkääjät hyödyntävät sitä. Vuonna 2014 OpenDNS Security Labs suoritti tutkimus kyselyn, jonka tuloksena lähes 67 % vastaajista ilmoitti, että he eivät seuraa rekursiivista verkkotunnus nimipalvelun liikehdintää haitallisen liikenteen varalta. Ciscon vuonna 2016 tekemän raportin mukaan yli 91 % hyökkäyksistä hyödyntää jollain tavalla verkkotunnus nimipalvelua. Verkkotunnus nimi palvelu on siis yleinen hyökkäys vektori myös aktiivihakemisto palvelimessa ja syytä pitää tietoturvallisena. (Lystrup 2016).

2.2 Aktiivihakemiston hyvät tietosuojakäytännöt

Organisaatioita suositellaan siirtymään salasanattomaan kirjautumiseen ja hyödyntämään kasvotodennusta, sormenjälkiä tai PIN-koodia. Sormenjälkeä ja PIN koodia suositellaan organisaatioille, joka ei voi vielä siirtyä kokonaan salasanattomaksi. Salasanan käytössä suositellaan salasanojen hallinta ohjelmistoa, joka luo vahvan satunnaistetun salasanan.

Organisaation tulee hallita harkitusti kokoonpanoasetuksia aktiivihakemistossa, koska väärin asetetuista kokoonpanoasetuksista voi tulla uusi hyökkäysvektori. Muutokset kannattaa toteuttaa muutoksen hallinta ohjelmistolla ja tarkastaa, ettei uudet muutokset avaa uusia hyökkäyspolkuja. Ennen muutoksia kannattaa aina varmistaa varmuuskopioinnin toimivuus 3-2-1 menetelmällä eli 3 kopiota alkuperäisestä + 2 varmuuskopiota kahdella eri tallennustyypillä ja 1 muualla tai ilman verkkoa oleva kopio. Hätäpalautus varmuuskopiot kannattaa olla kunnossa ja testattu, ennen kuin hyökkäävä taho pääsee tunkeutumaan organisaation järjestelmiin. (Microsoft 2020).

Normaalikäyttäjien pääsyä kannattaa rajata vain käyttäjän tarvitsemiin resursseihin. Käyttäjien oikeudet kannattaa jakaa ei enempää eikä vähempää periaatteella niin, ettei huonoimmassa tapauksessa hyökkääjä pääse lukemaan kaikkia organisaation tärkeitä tiedostoja vaan pienen osan niistä. Paikallisen tietokoneen järjestelmänvalvoja käyttäjätunnuksella tulee olla vahva salasana, koska sitä voidaan hyödyntää etäasennuksissa. Verkkotunnus nimipalvelun koko järjestelmänlaajuisten, järjestelmänvalvojan tason palvelutilien turhaa käyttöä kannattaa välttää. Verkonlaajuisen järjestelmänvalvojan tunnuksen avulla voidaan muuttaa suojausasetuksia, muuntaa tiedostoja, asentaa ohjelmistoja ja käyttää kaikkia verkkotunnus alueen tietokoneita. (Microsoft 2020).

Verkkopalveluiden segmentointi eli palveluiden hajautus useampaan järjestelmään hidastaa hyökkääjien etenemistä sisäverkossa. Verkostojen segmentointi rajoittaa hyökkäysten leviämistä ja antaa organisaatioille mahdollisuuden asettaa tiukempia valvontatoimia herkkien erillisjärjestelmien suojaksi. Segmentointi voi myös suojata päivittämättömiä järjestelmiä hyökkäyksiltä. Järjestelmän segmentoinnissa kannattaa ottaa käytäntöön Zero Trust ajattelutapa. Zero Trust ajattelutavassa ei oleteta, että kaikki organisaation palomuurin takana oleva liikenne olisi turvallista vaan tarkastetaan jokainen pyyntö ikään kuin se olisi peräisin ulkoverkosta. Zero Trust menetelmälle olennaista, että jokainen pyyntö on täysin todennettu, valtuutettu ja salattu ennen pääsyn myöntämistä järjestelmään. (Microsoft 2020).

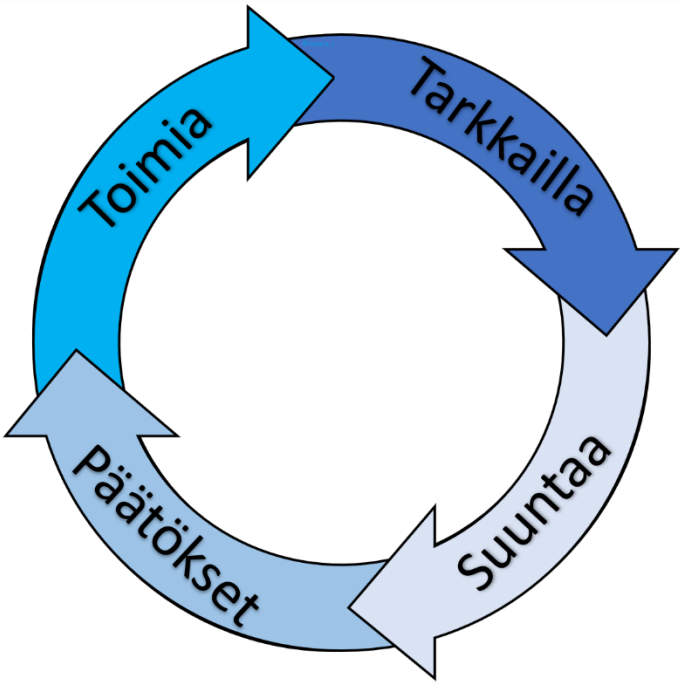
Aktiivihakemiston käytössä kannattaa hyödyntää käyttöoikeuksien analyysityökaluja. Näiden työkalujen avulla voidaan nopeasti ja helposti selvittää, mitkä oikeudet ja käyttöoikeusryhmät jollekin käyttäjälle on asetettu. Aktiivihakemistosta tarpeettomien käyttäjätilien tai oikeuksien säännöllinen poistaminen lisää järjestelmän tietoturvaa. Hylätyt tilit ovat kohde hyökkääjille, jotka etsivät passiivisia tilejä hyödyntääkseen organisaation luonnollista käyttäjätili suojaa. Varsinkin verkkotunnus järjestelmänvalvoja ryhmän käyttäjien määrä suositellaan pitämään mahdollisimman vähäisenä suojautuaksesi tältä mahdolliselta hyökkäykseltä. Yrityksen ICT-ryhmän tulee seurata irtisanomisia ja poistaa tai laittaa lukkoon kaikki ylimääräiset aktiivihakemisto tunnukset. (DNSstuff 2019).

3 Aktiivinen puolustus

Tietokoneiden käyttö on lisääntynyt vuosi vuodelta ja suurin osa järjestelmistä on nyt myös maailmanlaajuisen verkkoyhteyden päässä. Samalla kun järjestelmien ja ohjelmistojen monimutkaisuus kasvaa uusien ominaisuuksien mukana. Nämä kaikki lisääntyvät ominaisuudet järjestelmiin luo uusia haavoittuvuuksia, jota hyökkääjät voi hyödyntää. Aktiivisen puolustuksen tarkoituksena on pitää hyökkääjät järjestelmän ulkopuolella poistamalla haavoittuvuuksia nopeammin kuin hyökkääjät voivat löytää niitä. Aktiivisessa puolustuksessa korjataan jatkuvassa silmukassa mahdollisia heikkouksia järjestelmän tietoturvasta. Heikkouksien korjausta yritetään suorittaa mahdollisimman nopeasti ennen kuin hyökkääjät voivat hyödyntää niitä. (Goel & Mehtre 2015).

Tietojärjestelmän aktiivista puolustamista voisi kuvata englannin kielen sanonnalla ”game of cat and mouse”. Sanonta on keksitty viittaamaan kissan ja hiiren välistä suhdetta, jossa kissa ei pysty saamaan lopullista voittoa hiirestä, jos ei kykene saamaan sitä kiinni. Kun taas hiiren näkökulmasta huolimatta siitä, ettei hiiri kykene voittamaan kissaa se pystyy välttämään sieppauksen. Kissaa kuvaa tässä skenaariossa järjestelmän tietoturvaa vastaan hyökkäävä tahoa ja hiirtä kuvaa järjestelmän tietoturvan puolustaminen. Tietenkin tietoturvassa kissa voittaa jossain vaiheessa, kun järjestelmän tietoturva pettää. (Vogel 2019).

3.1 OODA-silmukka



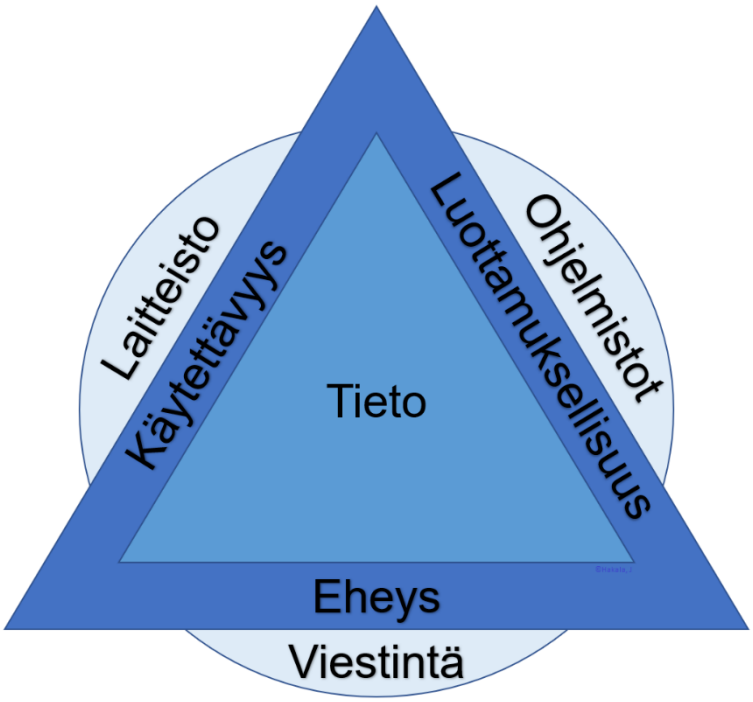
Kuva 2: Ooda-silmukka (Mukaillen VisualParadigm 2021)

OODA-silmukka menetelmä eli Observe, Orient, Decide ja Act tai suomeksi tarkkailla, suuntaa, päätökset ja toimet. Nelivaiheinen silmukka prosessi, joka on tarkoitettu päätöksien tekemisen tehostamiseen ja yhden asian tekemiseen todella hyvin. OODA-silmukka on alun perin kehitetty sotastrategian tueksi ja alkuperäinen kehittäjä on Yhdysvaltain ilmavoimien eversti John Boyd. Boyd sovelsi OODA-silmukka menetelmää taistelutoiminta prosessiin operatiivisella tasolla sotilaskampanjoiden aikana, mutta nykypäivänä se soveltuu erityisen hyvin kyberturvallisuuteen puolustavana tai hyökkäävänä menetelmänä. Prosessin on tarkoitus nopeuttaa päätöksentekoa ja toistaa uudestaan niin kauan, kunnes ongelmat saadaan korjattua. (Brehmer 2005). Ooda-silmukka kilpailee tässä tutkielmassa hyökkäysvaiheen Intrusion Kill Chain mallin kanssa, jolla etsitään järjestelmän heikkouksia. Mitä nopeammin OODA-silmukkaa suoritetaan, sitä turvallisempana järjestelmä saadaan pidettyä.

Ensimmäinen vaihe tarkkailu eli tiedon kerääminen mahdollisista ongelmista ja korjaus ehdotuksista. Tämän vaiheen tavoitteena on rakentaa mahdollisimman kattava kuva ongelmista. Jos tiedon perusteella halutaan tehdä hyviä päätöksiä sitä pitää katselmoida kokonaiskuvassa. Tietoa voidaan kerätä järjestelmän lokitiedoista, käyttäjä palautteesta, ohjelmistojen hallintapaneeleista tai ulkopuolisesta lähteestä. Silmukan toinen vaihe suuntaus, jonka tarkoituksena on tunnistaa kaikki esteet, jotka saattavat häiritä OODA-silmukan muita osia. Parhaat päätökset tehdään kohdentaen tarkasti aina ennen päätöksen tekemistä sen sijaan, että toimit liian nopeasti. Kolmas vaihe on päätöksentekovaihe, jolle kaksi ensimmäistä vaihetta tarjoaa tietoperustan tehdä tietoisia päätöksiä. Päätösvaiheen tarkoituksena on havaita edellisten vaiheiden virheet ja varautua niihin toiminta vaihetta varten. Silmukan viimeinen vaihe eli toiminta, jonka tarkoituksena on toimia kaikkien edellisten vaiheiden tiedon perusteella ja tulokset osoittavat oliko päätökset hyviä vai huonoja. Ooda-silmukan tarkoitus on tehdä päätöksiä nopeammassa rytmissä kuin vastustajat ja näin saavuttaa kilpailuetu vastaan hyökkäävään tahoon nähden. (FarnamStreet 2021).

Kun tietyllä tiedolla on päätöksentekovaiheessa negatiivinen merkitys, ihmiselle on luonnollista painottaa sitä liikaa positiivisen tuloksen rinnalla. Vastakohtana optimistinen puolueellisuus voi myös syrjäyttää negatiiviset seuraukset, jotka liittyvät tiettyyn tehtävään. Jos negatiivisella tai positiivisella tiedolla on suhteeton painoarvo analyysissä se voi vääristää tuloksia myös OODA-silmukka mallissa. On siis tärkeää pitää mielessä ihmiselle luonnolliset ennakkoasenteet päätöksentekoprosessin aikana. (Rieger 2021).

3.2 Tiedonkäsittely



Kuva 3: CIA-kolmio (Mukaillen Walkowski 2019)

Aktiivisen puolustuksen tarkoituksena on pitää organisaation tärkeät tiedot turvassa. CIA-kolmio eli confidentiality, integrity ja availability tai suomeksi luottamuksellisuus, eheys ja käytettävyys on aktiivinen tiedon suojelun malli. CIA-kolmion kolmea osaa pidetään tiedon tietoturvan tärkeimpinä elementteinä ja niiden tulisi olla organisaation tietoturvapäätöksissä mukana. Kolmiomalli on tarkoitettu ohjaamaan organisaation tiedon säilytystä koko elinkaaren vaiheissa säilytyksessä, siirtämisessä, hyödyntämisessä ja tuhoamisessa. Tiedon luottamuksellisuudessa olennaista estää luvattomilta henkilöitä luottamuksellisiin tietoihin pääsy. Luottamukselliset tiedot voidaan luokitella niiden herkkyyden mukaan ja suojata erilaisilla salausmenetelmillä. Tiedon eheydelle välttämätöntä, että tiedon luottamuksellisuus on kunnossa. Tiedon eheydelle olennaista, ettei luvattomat henkilöt pääse muokkaamaan tiedostoa ilman lupaa. Tiedoston eheyttä voidaan turvata käyttöoikeuksilla, versionhallinnalla ja pääsynvalvonnalla. Tiedon käytettävyydellä tarkoitetaan sitä, että valtuutetut henkilöt voivat käyttää tiedostoja helposti luottamuksellisuus ja eheys toimenpiteistä huolimatta. Käytettävyydelle ominaista, että tiedot ovat myös pahimmassa tapauksessa palautettavissa varmuuskopioista. Kolmiomallin tietoturvallisuus toimii kokonaisuutena ja yhtään osaa ei voida jättää pois ilman, että se vaikuttaisi toisiin osiin. (Tyson 2019).

Tietojärjestelmät koostuvat kolmesta elementistä laitteisto, ohjelmistot ja organisaation sisäisestä viestinnästä. Tietojärjestelmän pitäminen turvallisena avustaa myös tiedon tietoturvan ylläpitämisessä. Todennus- ja tunnistusmenetelmät tapahtuvat järjestelmien ohjelmistojen avulla. Tietoturvalliset laitteistot, ohjelmistot ja käyttäjä viestintä on suuressa

osassa tärkeiden tiedostojen turvassa pitämisessä. (Stewart, Chapple & Gibson 2012, 477–530).

Tiedon säilytyksessä on tärkeää, että tiedon elinkaari hoidetaan kunnolla tiedon syntymästä tiedon kuolemaan. Kaikkiin tiedon elinkaariin kuuluu tiedon kerääminen, säilytys, käyttö ja hävitys. Tieto pitää säilyttää turvallisesti kaikissa näissä vaiheissa, ettei se päädy luvattomille henkilöille hyödynnettäväksi. Kun tietoa ei enää käytetä se pitää myös tuhota tai arkistoida tietoturvallisesti. (Reiner, Press, Lenaghan & Barta 2004).

3.3 Riskienhallinta

Riskienhallinta on tärkeää, jotta riskit voidaan ennaltaehkäistä tai huonoissa tapauksissa riskeistä voidaan elpyä nopeasti. Tietoturvariskinä nähdään asiat, jotka voi haitata tai viivästyttää organisaation toimintaa. Vaarana riskienhallinnassa on se, ettei toimintaa uhkaavia riskejä tunnisteta ajoissa ja ulkopuolinen toimija pääsee hyödyntämään organisaation tietoturvan heikkouksia. Tietoturvariskejä voidaan tunnistaa organisaation määrittämän riskienhallintaryhmän toimesta tai käyttäjien esiin tuomista ongelmista. (Valtiovarainministeriö 2017).

Kun riski tunnistetaan, sen ominaisuudet kuvataan mahdollisimman tarkasti korjausta varten. Tunnistetut riskit voidaan arvioida riskin suuruuden ja uhkan toteutumisen todennäköisyyden avulla. Riskin suuruuden ja uhkan toteutumisen todennäköisyyden avulla saadaan parempi kuva riskistä ja miten se voidaan estää. Kaikkia riskejä ei tietenkään voi poistaa kokonaan, mutta niiden mahdollisia tapahtuma kertoja voidaan yrittää vähentää. Löydetyille riskeille tehdään sopivat toimenpiteet, joita on välttäminen, pienentäminen, siirtäminen tai parhaassa tapauksessa poistaminen. Riskien kartoituksessa kannattaa ottaa myös huomioon kaikki organisaation järjestelmät kuten käyttäjien omat tietokoneet, koska ne voi toimia välihyppynä tärkeisiin palvelimiin. (Valtiovarainministeriö 2017).

3.4 Tietoturva poikkeuksien selviytymissuunnitelma

Tietoturva poikkeuksien selviytymissuunnitelma on kriittinen osa organisaation tietoturvasta, koska mikään järjestelmä ei takaa absoluuttista tietoturvaa. Toipumissuunnitelman tarkoituksena on kehittää organisaation toipumista tietoturva poikkeustilanteista takaisin normaalitilaan mahdollisimman nopeasti. Katastrofeista toipuminen on yleisesti riippuvainen riskienhallintaprosessista, jossa riskit pyritään ehkäisemään. Katastrofista toipumisen suunnittelu voi myös johtaa katastrofin välttämiseen ja se vahvistaa organisaation kykyä reagoida tietoturva poikkeuksiin. (Valtiovarainministeriö 2017).

Tietoturva toipumissuunnitelmat on tärkeitä yrityksen liiketoiminnan jatkuvuuden turvaamiseksi. Tietoturva poikkeuksien toipumistoimenpiteisiin kannattaa varata aikaa ja resursseja, ettei tietoturvaongelma uusiudu. Toipumissuunnitelman toimivuus kannattaa myös varmistaa käytännössä ennen oikeaa tietoturvapoikkeus tilannetta. Toipumissuunnitelman ensimmäinen vaihe löytää miten järjestelmä on saastunut ja tukkia järjestelmän haavoittuvuudet. Jos hyökkääjä on päässyt johonkin järjestelmään sisälle saastunut järjestelmä kannattaa asentaa kokonaan uudelleen, koska hyökkääjältä voi jäädä epätoivottuja ohjelmistoja järjestelmään. Järjestelmässä kirjautuneiden tai hyödynnettyjen tunnuksien salasanat vaihdetaan uuteen tietoturvalliseen salasanaan. Kun järjestelmä ja tunnukset on todettu turvalliseksi, voidaan aloittaa tiedostojen palauttaminen varmuuskopioista. Viimeinen vaihe on kehittää tietoturvan toimintatapoja turvallisempaan suuntaan. (Valtiovarainministeriö 2017).

Tietojen varmuuskopioinnin tarkoituksena on mahdollisten taloudellisten menetysten minimointi ja tietojen suojaaminen häviämiseltä. Tietoturvaongelma tilanteessa parhaassa tapauksessa yrityksen tärkeät tiedot ei katoa eikä yksityiset tiedot vuoda julkisuuteen. Huonoimmassa tapauksessa kaikki tärkeät tiedot katoavat ja yksityiset tiedot vuotavat julkisuuteen. Varmuuskopiointi kannattaa siis suorittaa huolella ja tietoturvallisesti. Tärkeistä tiedostoista ja järjestelmistä kuuluu ottaa varmuuskopiot paikallisesti sekä etäsijaintiin. Kopioita tulee olla vähintään 3 jos tiedot ovat tärkeitä. Varmuuskopiot säilytetään eri paikassa, kun alkuperäiset tiedostot, ettei alkuperäinen tietoturvapoikkeus vaikuta myös niihin. Tietojen palautuksen toimivuus varmuuskopiosta kannattaa testata kokeilemalla ennen poikkeustilanteita, että ne toimivat oletetusti. Varmuuskopiot tulee säilyttää tietoturvallisesti, koska niistä voidaan saada tietoa hyökkäystä varten. (Al-Ansary 2014).

3.5 Tunkeutumisen havaitsemisjärjestelmä ja tunkeutumisen ehkäisyjärjestelmä

Tunkeutumisen havaitsemisjärjestelmä valvoo verkkoliikennettä ja tunnistaa epänormaalin tilanteen normaalista. Tilanteen mukaan järjestelmällä voidaan havaita monenlaisia epänormaaleja tilanteita, kuten tietoturvakäytäntöjen rikkomukset, haittaohjelmat ja porttiskannerit. Havaitsemisjärjestelmälle tyypillistä, ettei se tee itse toimintoja havaintojen perusteella vaan lähettää hälytyksen eteenpäin seuraavalle järjestelmälle tai ihmiselle. (Petters 2020).

Tunkeutumisen ehkäisyjärjestelmä tekee automaattisesti hyökkäyksen estämistoiminnot ja toimii yleisesti yhteistyössä liikenteen estävien järjestelmien ja tietoturva poikkeuksien havaitsemisjärjestelmän kanssa. Tunkeutumisen ehkäisyjärjestelmän tarkoitus on tunnistaa vaarallinen paketti ja pudottaa se ennen kuin hyökkäys saavuttaa tavoite toimenpiteensä. Näiden järjestelmien tehtävänä on lopettaa hyökkäyksiä ennen kuin ne leviävät

laajemmin organisaation sisäverkossa. (Petters 2020). Näiden järjestelmien hankinnassa kannattaa tarkastaa palveluntarjoajan luotettavuus historia.

3.6 Aktiivihakemiston On-Demand arviointi

Järjestelmän On-Demand arviointi on tärkeä lisäys aktiivihakemiston tietoturvaan, että organisaation palvelimen turvallisuudesta saadaan parempi kokonaiskuva. Arviointijärjestelmä auttaa organisaation ICT-tiimiä ymmärtämään ympäristönriskit, ympäristön terveyden ja miten ympäristöä voidaan parantaa tietoturvaan katsottuna. Microsoft tarjoaa myös ammattilaisten arviointipalvelua, jossa Microsoftin oma insinööritiimi arvioi organisaation itse asentaman palvelimen. Arviointiprosessiin kuuluu mm. Toimintaprosessien tarkastus, ryhmien/käyttäjien oikeuksien tarkastus, verkkotunnus alueen tarkastus, käyttäjä identiteetinhallinta ja toimialue ohjaimen asetuksien tarkastus. Hyötynä organisaatio saa asiantuntija analyysin suoraan Microsoftilta ja voi kehittää palvelimen tietoturvaa organisaatiolle räätälöidyn ohjeistuksen avulla. (Microsoft 2019).

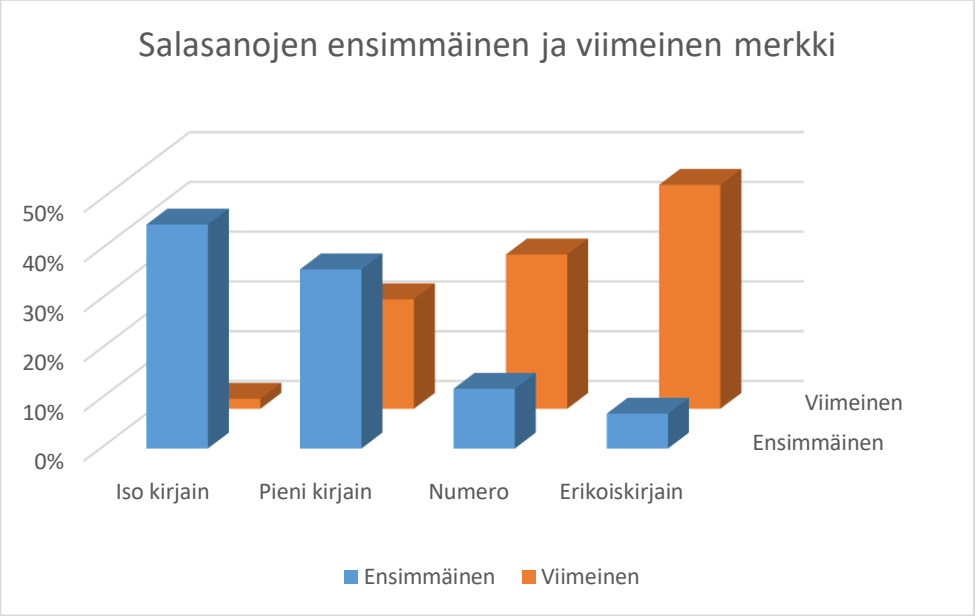
4 Loppukäyttäjien vastuut aktiivisessa puolustuksessa

Yleisinä sääntöinä organisaation laitteiden, sovelluksien ja verkkojen käytössä on, että kaikki käyttäjät vastaavat omista tunnuksistaan henkilökohtaisesti. Käyttäjä on siis vastuussa käyttäjänimensä kaikesta käytöstä eikä tunnuksia saa antaa muiden käyttöön. Käyttäjätunnus suositellaan suojaamaan vahvalla salasanalla ja muuten ohjeistetulla tavalla, kuten kaksivaiheisella todennuksella. (Haaga-Helia 2014).

Toinen yleinen merkittävä käyttäjän vastuulla oleva asia on saatuaan itselleen arkaluonteisen tai ulkopuolisilta salatun tiedoston, käyttäjän tulee suojata tiedostoa asianmukaisesti. Arkaluonteisten tietojen lähettäminen pitää hoitaa organisaation ohjeistamalla tavalla niin, ettei ulkopuoliset tahot voi lukea tiedostoa. (Perelman 2014).

4.1 Salasanat

Taulukko 1: Salasanojen yleiset muotoilut (mukaillen Abbott & Garcia 2015)



Käyttäjien salasana käytännöissä on parantamisen varaa monella tavalla ja käyttäjiä pitäisi kouluttaa hyviin salasana käytäntöihin. Taulukko 1 kuvattu N&N Global Technologyn vuonna 2015 tekemän tutkielman tuloksia, käyttäjien salasanojen ensimmäisestä ja viimeisestä merkistä. Tutkimuksesta selvisi myös suosituin erikoismerkki, joka oli huutomerkki. Käyttäjille oli pakotettu salasanan luomisvaiheessa, että salasanan pitää sisältää vähintään yksi numero, erikoismerkki, iso kirjain ja pieni kirjain. (Abbott & Garcia 2015). Tästä voidaan päätellä monen käyttäjän muuntavan vanhoja salasanoja uusiin huonolla tavalla esim. Huonoksi todettu vanha salasana password123 muunnetaan Password123!.

Jos käyttäjältä löytyy vanhoja salasanoja julkisesti vuotaneista salasanalistoista ja käyttäjä vaihtaa salasanan esimerkin mukaisesti salasana on vieläkin helposti arvattavissa.

NCSC:n vuonna 2018 tekemän tutkimuksen mukaan kaikista tutkimukseen osallistuvista organisaatioista 75 prosentilla oli käyttäjiä, jonka salasanoja löytyi tuhannen parhaan salasanan joukossa ja 87 prosentilla oli käyttäjiä, jonka salasanoja löytyi 10 000 parhaan joukosta. Tämä altistaa käyttäjiä salasanan arvaus hyökkäykselle. Tehokkain tapa torjua salasanan arvaaminen on estää käyttäjiä käyttämästä huonoja salasanoja. Käyttäjille tulee myös antaa käytännön neuvoja, kuinka valitaan hyvät salasanat. Käyttäjätunnuksien väärinkäytön voi estää ottamalla kaksivaiheinen todennus käyttöön pakotetusti koko organisaation laajuisesti ja luoda ehdollinen pääsy järjestelmiin. Microsoftin järjestelmien kautta voidaan säätää ehdollinen pääsy esimerkiksi vain niille käyttäjille, jotka kirjautuvat yrityksen sisäverkosta. Järjestelmänvalvoja voi myös rajata salasanan kokeilukertoja hidastaakseen salasanan arvaus hyökkäystä, mutta tämä ei ole paras ratkaisu tähän ongelmaan. (National Cyber Security Centre 2018).

Mitä kauemmin käyttäjällä on sama salasana, sitä suurempi mahdollisuus hyökkääjällä on löytää salasana. Ennestään käytetyn salasanan voi löytää vanhoista vuotaneista salasanalistoista selkokielisenä tai salatussa muodossa. Salasanan murtamisen riski kasvaa, jos salasana on huono ja sitä ei vaihdeta pitkään aikaan. Tietenkin vaarantuneen käyttäjän tunnukset ovat hyökkääjän hyödynnettävissä, kun salasanat jätetään vaihtamatta. Uuden salasanan kuuluu olla ainutlaatuinen, siksi salasanan vaihdossa kannattaa myös pakottaa salasanan historiallinen tarkastus. Salasana ei saa olla liian lyhyt tai se joutuu sanakirjahyökkäyksen kohteeksi. Erittäin pitkiä salasanoja ei myöskään suositella, koska käyttäjä saattaa ottaa salasanan ylös johonkin epävarmaan paikkaan. Liian pitkät salasanat usein kirjoitetaan myös väärin ja tunnukset lukittuvat, tämä voi ruuhkauttaa yrityksen IT-tukea turhaan. (CIS 2020).

4.2 Loppukäyttäjien koulutus

Käyttäjien tietoturvakoulutus on tärkeä asia, koska käyttäjät ovat usein järjestelmän tietoturvan suurin riski. Kaikkien käyttäjien pitää vähintään huolehtia oman käyttäjätunnuksen turvallisuudesta. Jos käyttäjiä koulutetaan ja tiedostetaan tietoturvariskeistä paremmin, tietojenkalastelu hyökkääjien onnistumismahdollisuudet huononevat. Käyttäjien tulisi vähintään tunnistaa huijausyritykset sähköpostissa, puhelin soitoista ja tekstiviesteissä. Käyttäjiä voidaan myös testata lähettämällä organisaation sisäinen testi huijausviesti ja tiedottaa tietoturvariskeistä testauksessa kiinnijääneitä käyttäjiä. Koulutus tilanteissa on hyvä näyttää tyypillisiä esimerkki huijausviestejä ja niiden ominaisuuksia käyttäjille. (Kyberturvallisuuskeskus 2019)

5 Mahdolliset hyökkäykset palvelimelle

5.1 Kuka hyödyntää aktiivihakemiston haavoittuvuuksia?

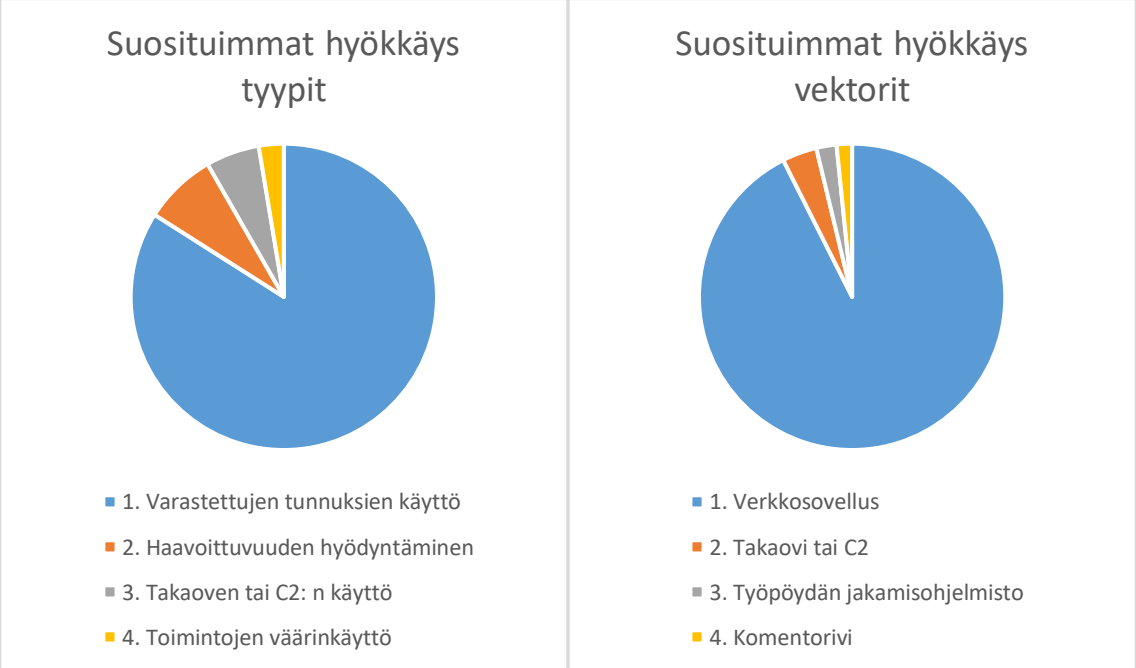
Verizonin tekemän tiedonkeruun mukaan yli puolet kaikista onnistuneista hyökkäyksistä suorittaa järjestäytyneet rikollisryhmät. Järjestäytyneen rikollisryhmän kohteeksi joutuminen on todennäköisesti pahin mahdollinen tapaus, koska heitä ei yleisesti kiinnosta mitä organisaation tiedoille ja palvelimille tapahtuu hyökkäys prosessin aikana tai jälkeenpäin. Organisoidun rikollisuuden hyökkäyksien motivaatio on lähes aina taloudellinen, kun rikollinen saa organisaatiolta tietoja haltuun niitä hyödynnetään kaikin keinoin. (Verizon 2020).

Kerätystä tiedosta tulee ilmi se, että onnistuneissa hyökkäyksissä on mukana myös loppukäyttäjiä ja järjestelmänvalvojia, jotka tekevät huolimattomia virheitä. Osan onnistuneista hyökkäyksistä voi siis tulla organisaatioon palkatun henkilön kautta. Motivaationa tähän voi olla rikollisryhmän tarjoama maksu käyttäjälle, törkeä huolimattomuus tai kosto yritys. (Verizon 2020).

Tietenkin myös valtioiden välinen vakoilu löytyy yleisimpien hyökkääjien listalta. Valtioiden tukemat hyökkäykset kohdistuvat yleisesti toiseen valtion virastoon tai suuriin yrityksiin. Parhaassa tapauksessa organisaation palvelimelle hyökkäys onnistuu vain organisaation itse palkkaaman eettisen hakkerin toimesta, joka voi ohjeistaa tietoturvariskin korjauksessa. (Verizon 2020).

5.2 Yleiset hyökkäystavat

Taulukko 2: Verizon suosituimmat hyökkäykset (mukaillen Verizon 2020)



Kaikki hyökkäykset voidaan jakaa kolmeen ryhmään varastettujen tunnuksien käyttäminen, haavoittuvuuksien hyödyntäminen ja takaovet. Verizonin keräämistä tiedoista voidaan päätellä, että suurin osa onnistuneista hyökkäyksistä on varastettujen tunnuksien hyödyntämistä verkkosovelluksien kautta. Kerättyjen tietojen perusteella yksi hyvä tapa vähentää hyökkäyksiä on siirtää hyökkäys pintaa useaan eri palvelimeen, kuten verkkosovelluksien siirtäminen kokonaan omalle palvelimelle ja erilliseen verkkoon tai pilvipalveluun. Riskialttiita verkkosovelluksia ovat varsinkin ne joihin käyttäjät voi itse ladata jotain, kuten kuvia tai muita tiedostoja. (Verizon 2020).

Varastettujen tunnuksien hyödyntäminen hakkeroinnissa on ollut nousussa, koska se on helposti hyödynnettävissä vuotaneiden tunnuksien avulla. Kerätyistä tiedoista nähdään myös se, että organisaatiot käyttävät paljon aikaa haavoittuvuuksien korjaamiseen ja järjestelmien päivitykseen, siksi suhteellisen pieni osa haavoittuvuuksista päätyy onnistuneen hyökkäyksen kohteeksi. (Verizon 2020).

5.3 Aktiivihakemisto palvelimeen yleisesti kohdistuvia hyökkäyksiä

Verkkotunnus ohjain synkronisointi hyökkäyksessä väärinkäyttäjä hyödyntää verkkotunnusten ohjaimen käyttäjätunnusta saadakseen käyttäjien todennustietoja palvelimelta. Hyökkääjä saa todennustiedot palvelimesta esittämällä itse olevansa verkkotunnus ohjain järjestelmäkäyttäjä. Tämä hyökkäys vaatii sen, että hyökkääjä on saanut etuoikeutetun käyttäjätunnuksen aktiivihakemisto palvelimessa käyttöön tai verkkotunnus ohjaimen järjestelmäkäyttäjää voidaan hyödyntää haavoittuvuuden avulla. (Van Cott 2020).

LDAP-protokollan tiedustelu hyökkäyksessä väärinkäyttäjä tiedustelee Microsoftin käyttämää LDAP-protokollaa ulkoa käsin. Väärinkäyttäjä luo omia kyselyitä LDAP-protokollalle ja saa vastauksena tietoa verkkonimi alueen käyttäjistä, ryhmistä ja tietokoneista. Hyökkäyksen tarkoituksena kerätä tietoja, jota käyttää jalansijan saamisessa järjestelmään. (Stealthbits Technologies 2021).

Pass-to-hash hyökkäyksessä väärinkäyttäjä on saanut tiedustelu vaiheessa haltuun salatun salasanan, jota ei ole onnistunut purkamaan. Hyökkäystyökalun avulla väärinkäyttäjä saa salasanan syötettyä järjestelmään salatussa muodossa ja pääsee suorittamaan käyttäjällä toimintoja. Tämän hyökkäyksen tavoitteena on päästä kirjautumaan käyttäjätunnuksella ja edetä järjestelmässä. Tämä hyökkäys toimii vain, jos järjestelmässä on käytössä sama salaustekniikka, kun väärinkäyttäjän haltuun saamassa salatussa salasanassa. (BeyondTrust 2020).

6 Palvelimelle hyökkäys

Tutkielman hyökkäyksien kokeiluvaiheessa käytetään oikeita hyökkäyksiä koulutustarkoituksessa, nämä hyökkäykset ovat laittomia väärinkäytettyinä. Menetelmiä saa käyttää vain sallittuihin kohteisiin, jonka itse omistat tai olet saanut kirjallisen luvan tehdä tunkeutumistestausta.

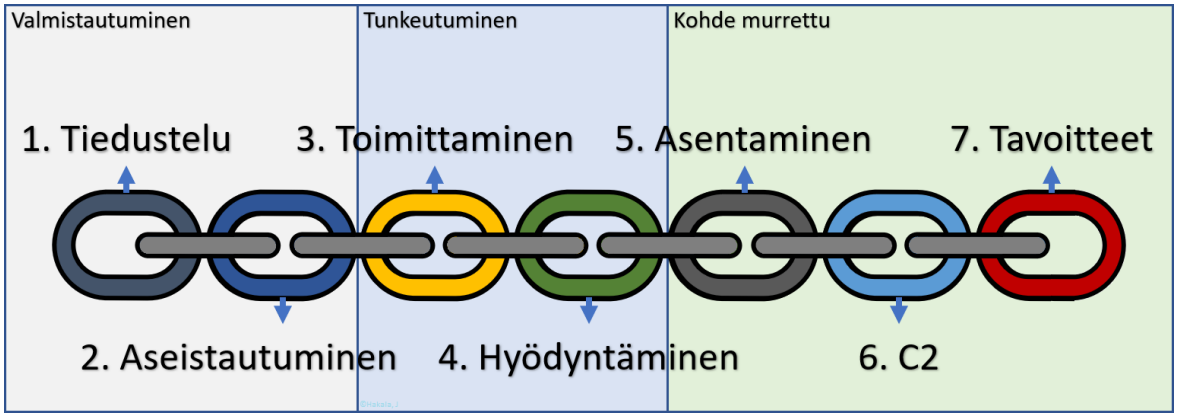
Suomen rikoslain 19.12.1889/39, 38 luvun tieto- ja viestintärikoksista 10.4.2015/368 8 § mukaan:

> ”*Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.*” (Finlex 2015.)

Hyökkäysvaiheessa käytetään valkoisen laatikon testausta eli hyökkääjä tietää kaiken kohteesta. Valkoisen laatikon testauksessa olennaista, että hyökkääjällä on tietoa käynnissä olevista sovelluksista, versioista, käyttöjärjestelmästä, lähdekoodeista, arkkitehtuurista ja verkoista. Valkoisen laatikon menetelmässä hyökkäyksen avulla saadaan kattavin arviointi ulkoisista ja sisäisistä heikkouksista, koska myös järjestelmän sisäinen tietoturvan tutkiminen on taattu tässä menetelmässä. (Poston 2020).

Palvelimelle ei ole asetettu kunnon tietoturvatoimenpiteitä, koska tämän vaiheen tarkoituksena on havainnollistaa hyökkäykset alusta loppuun eikä estää niitä. Hyökkäyksien avulla saadaan parempi kuva siitä, miksi aktiivihakemisto palvelimen parhaat käytännöt, palvelimen päivitys ja oikeat asetukset ovat tärkeitä.

6.1 Intrusion Kill Chain



Kuva 4: Tunkeutumisen tappoketjun vaiheet (mukaillen Sławińska 2020)

Intrusion kill chain eli suomeksi tunkeutumisen tappoketju, jonka on alun perin kehittänyt Lockheed Martin, Military Kill Chain mallin perusteella. Military Kill Chain malli on suunniteltu armeijan hyökkäys malliksi löytää, taistella ja voittaa vihollinen. Nykypäivänä vanhat armeija taktiikat ovat sovellettavissa erityisen hyvin kyberturvallisuuteen. Lockheed Martin kyberhyökkäys malli tunkeutumisen tappoketju sisältää seitsemän kuvan 4 mukaista vaihetta tiedustelu, aseistautuminen, toimittaminen, hyödyntäminen, asentaminen, C2 ja tavoitteet. Mallia käytettäessä hyökkäykseen tarkoituksena on päästä viimeiseen vaiheeseen tekemällä ensimmäisestä vaiheesta eteenpäin järjestyksessä. Jos hyökkääjä pääsee viimeiseen vaiheeseen tekemään tavoitteiden mukaisia toimenpiteitä, voidaan todeta järjestelmän saastuneen kokonaisuudessaan. Viimeisen vaiheen yleinen tarkoitus organisoiduille rikollisryhmille on järjestelmän ja sen tietojen kaupallistaminen omaksi hyödykseen. Lockheed Martin alkuperäisessä ohjeessa tunkeutumisen tappoketjua hyödynnetään puolustavana menetelmänä, mutta tässä tutkielmassa käytämme sitä hyökkäyksien harjoittelussa ja havainnollistamisessa. (Hutchins, Cloppert & Amin 2010). Tässä tutkielmassa tunkeutumisen tappoketju mallin vastakohtana, toimii OODA-loop puolustavana menetelmänä ja nämä kaksi menetelmää kilpailee toistensa kanssa. Mitä nopeammin toinen näistä menetelmistä toimii sitä parempi kilpailuetu sillä, on toiseen menetelmään nähden.

Tunkeutumisen tappoketjua voidaan siis käyttää myös puolustavasti arvioimalla hyökkäyksen ominaisuuksia ja mihin vaiheeseen tunkeutumisen tappoketjussa hyökkäys on edennyt. Järjestelmän tietoturvaa voidaan korjata tarkastelemalla mihin vaiheeseen hyökkäys on edennyt ja tulkita tunkeutumisen tappoketjua takaperin. Takaperin tulkitsemisen tarkoituksena korjata järjestelmän haavoittuvuuksia jokaiselta tunkeutumisen tappoketjun vaiheelta, johon hyökkääjä on päässyt. Kaikki vaiheet, joita hyökkääjä hyödyntää on tärkeä korjata ja dokumentoida, ettei hyökkäykset ole toistettavissa. Tunkeutumisen tappoketjun avulla voidaan luoda mahdollisimman realistinen hyökkäysskenaario, jossa järjestelmät voivat näyttää toimivansa. (Lockheed Martin Corporation 2015).

6.2 Hyökkäykset tunkeutumisen tappoketjun eri vaiheissa

Järjestelmän puolustuksessa tulee myös ottaa huomioon, miten hyökkääjät ajattelevat. Puolustavan tahon tulee ottaa selvää mitkä palvelut ovat arvokkaita suojata, koska jos tärkeää järjestelmää ei tunne tai ymmärrä sitä on haastavaa suojata. Tärkeät järjestelmät yleisesti sisältävät tärkeitä tietoja tai menetelmän edetä hyökkäyksessä. Hyökkääjät voi priorisoida tiettyjä järjestelmiä tai tilejä, koska niillä on oikeus laajempiin resursseihin järjestelmissä. (Microsoft 2016).

Tämän vaiheen tarkoituksena on tehdä hyökkäyksiä tunkeutumisen tappoketjun eri vaiheissa ja havainnollistaa miten hyökkäykset toimivat käytännössä. Hyökkäyksien havainnollistamisella opitaan hyökkääjän ajattelu tapaa, jotta järjestelmien puolustamisesta tulee selkeämpää. Hyökkäyksiä on vaikea estää, jos ei tiedetä minkä kaltaisia hyökkäyksiä järjestelmää vastaan voidaan oikeasti toteuttaa. Hyökkäyksien tarkka dokumentointi on tärkeää tunkeutumistestauksen jokaisessa vaiheessa, ettei samoja hyökkäyksiä suoriteta turhaan monta kertaa ja puolustavan tahon kanssa voidaan myöhemmin katsoa mitä on tehty ja mihin aikaan. Hyvin tehdystä dokumentaatiosta on myös apua silloin kun tehdään maksettua hyökkäystestausta, koska on myös tärkeä tarkastaa, onko kohde organisaatio huomannut hyökkäykset.

6.2.1 Tiedustelu

Tiedustelu vaihe on valmistautumisen ensimmäinen vaihe, jonka avulla etsitään järjestelmästä alustavia heikkouksia ja saadaan parempi ymmärrys kohteesta. Tiedustelu on tärkeä osa onnistuneessa hyökkäyksessä ja siihen käytetään kokonaiskuvaan katsottuna todella paljon aikaa. Tiedustelu vaihe kannattaa suorittaa kunnolla, koska myöhempien vaiheiden hyökkäykset suoritetaan tiedustelun avulla tehtyjen löydösten perusteella. Tiedustelusta kannattaa pitää kirjallista dokumentointia, johon palata lisätietoja tarvittaessa. Myös tiedustelu vaiheessa hyvä ottaa huomioon, että jotkin järjestelmän tiedustelutavat voi olla laittomia. (Hutchins ym. 2010).

Yleinen tapa aloittaa tiedustelu vaihe on porttiskannaus, että saadaan tietoa järjestelmistä ja avonaisten porttien ohjelmistoista. Porttiskannaus voidaan suorittaa, jos palvelimeen saadaan verkkoyhteys IP-osoitteella. Porttiskannauksen suoritus voi kestää kauan aikaa riippuen palvelimen ohjelmistoista ja verkon laajuudesta eli se kannattaa laittaa taustalle pyörimään muuta tiedustelua suorittaessa. Aktiivihakemisto palvelimen porttiskannauksessa käytetty nmap porttiskannaus ohjelmaa lipulla -sC oletusarvoinen komento skripti tarkastukselle ja lippulla -sV tunnistaa palveluiden versiot. Komento suoritetaan palvelimen sisäverkon osoitteelle 192.168.10.120. (die.net 2011). Porttiskannaus kokonaisuudessaan ”Liite 1. Nmap porttiskannaus”. Porttiskannauksesta saadaan tietoon avoimet portit, verkkotunnus alueen nimi, palveluiden nimet ja ynnä muuta tietoa. Tietojen perusteella voidaan päätellä, että kyseessä aktiivihakemisto palvelin, jossa verkkotunnus toimialueen nimi dunttus.

Tiedustelu vaiheessa voidaan etsiä huonosti säilytettyjä tiedostoja kuten vanhan käyttöjärjestelmän varmuuskopiot, josta voidaan ottaa talteen Windows käyttöjärjestelmän paikallisesti tallentamia käyttäjätunnuksia ja salasanoja. Windows salasana tiedoston NTLM-salaus voidaan purkaa tai käyttää salatussa muodossa kirjautumiseen. Jos salasanoja ei olla vaihdettu varmuuskopioinnin jälkeen, hyökkääjä voi kirjautua käyttäjätunnukselle.

Aktiivihakemisto palvelun kautta autentikoidaan organisaation käyttäjille resursseja eli tässä vaiheessa voidaan myös etsiä käyttäjätunnuksia. Organisaation kotisivujen henkilöstösivut ovat hyvä paikka etsiä mahdollisia käyttäjätunnuksia. Yleinen tunnuksien muotoilu on sama kuin sähköpostissa eli etunimi.sukunimi, jolle voidaan yrittää arvata salasana. Nämä samat tunnukset käyvät yleisesti myös Outlookin sähköpostiin, koska niitä hallinnoidaan aktiivihakemiston kautta. Julkisesti vuotaneet käyttäjä/salasanalistat ovat hyviä työkaluja etsiä vanhoja salasanoja, joiden avulla arvata käyttäjien nykyinen salasana. Huonojen tietoturvakäytäntöjen omaavien käyttäjien tilejä voidaan myös, yrittää saada sosiaalisilla tietojenkalastelu hyökkäyksillä sähköpostitse, tekstiviestillä tai puhelulla. Tiedustelua voidaan myös tehdä kaikesta organisaation julkisesta materiaalista esim. Kyseisen organisaation avoimien työpaikkojen kautta, joissa yleisesti ilmoitetaan minkä järjestelmän osaamista tarvitaan. Tiedustelussa voidaan hyödyntää fyysistä tiedustelua, johon kuuluu esim. Huonosti lukitut ovet ja kulkeminen ilman lupaa, mutta tässä tutkielmassa ei paneuduta fyysiseen tiedusteluun tätä tarkemmin.

6.2.2 Aseistautuminen

Toinen valmistautumisen vaihe aseistautuminen, jossa tiedustelu vaiheen perusteella hankitaan työkaluja seuraavaa vaihetta varten. Työkalut voivat olla myös käyttäjätunnuksia, jonka avulla saada alustava jalansija järjestelmään. Kali Linux tarjoaa monta eri ohjelmaa etsiä haavoittuvaisuuksia ohjelmistojen eri versioista ja monesti näille haavoittuvuuksille on valmiiksi tehtyjä hyötykuormia. Haavoittuvuuksia voidaan myös etsiä suoraan verkon hakukoneista, ohjelmiston lähdekoodista tai vanhan version ohjelmistoista suoraan ohjelmiston valmistajan muutoslokista. (Hutchins ym. 2010).

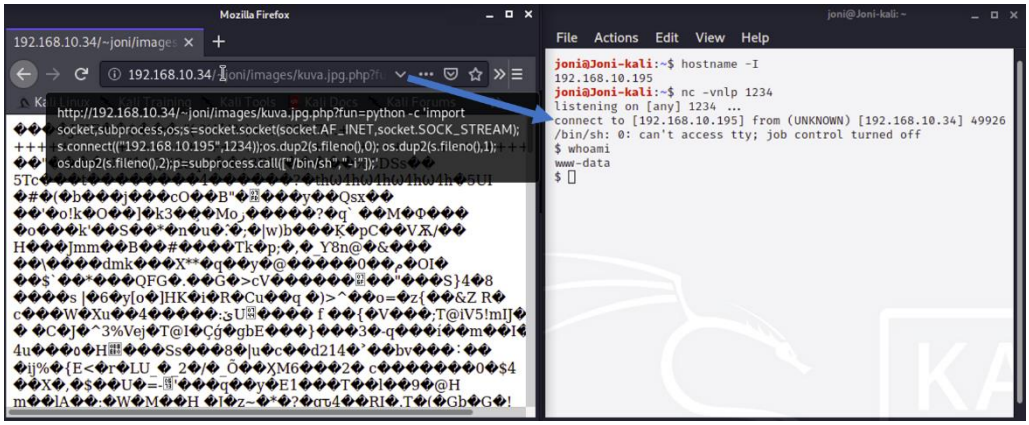
Päivittämättömään Windows palvelimeen toimii ZeroLogon haavoittuvaisuus hyötykuorma, jota voidaan hyödyntää Impacket hyökkäys kirjaston ja EvilWinRm etäkonsoli ohjelman avulla. Seuraavissa vaiheissa käytetään aseistautumisvaiheessa hankittuja ohjelmistoja ja haavoittuvaisuus hyötykuormia.

6.2.3 Toimitus

Toimitusvaiheessa aloitetaan hyökkäyksen toimituksen suunnittelu, jossa etsitään toimitustapa tiedustelu vaiheessa löydetylle tietoturvariskille. Toimitusvaihe voi olla onnistumisesta riippuen todella hidas tai nopea vaihe. Hyökkäyksen toimituksena voi toimia tietoliikenne, verkkosivut, epäluotettava työntekijä tai konkreettinen toimitus. Hyökkäävä taho voi myös saada jalansijan samassa sisäverkossa olevasta järjestelmästä ja hyödyntää sitä toimitustapana kohde järjestelmään. (Hutchins ym. 2010).

Verkkosovelluspalvelimen hyödyntäminen voi toimia välihyppynä aktiivihakemisto palvelimeen, joka toimii organisaation sisäverkossa. Jos sisäverkkoa ei olla segmentoitu riittävästi aktiivihakemisto palvelimeen voidaan saada suora yhteys. Suurin riski verkkosovelluksissa on antaa käyttäjien ladata tiedostoja kuten kuvia palvelimelle, koska näitä latauksia on vaikeaa suodattaa virheettömästi. Verkkosovelluspalvelin oli myös suosituin onnistuneiden hyökkäyksien kohde Verizonin keräämän tiedon perusteella. Seuraavaksi toteutetaan nopea demonstraatio PHP-verkkosovellus palvelimeen jalansijan saamisesta.

Kuva tiedostoihin voidaan lisätä metatietoja, joka voi olla myös haittakoodia. Ensin Exiftool ohjelmalla lisätään omia metatietoja kuva tiedostolle, metatietoa lisätään terminaali komennolla: exiftool -Comment='<?php echo system($_REQUEST['fun']); ?>' kuva.jpg. Kuvaan lisättiin metatieto riville -Comment PHP-haittakoodia, joka mahdollistaa koodin etäsuorituksen selaimen kautta funktiolla ”fun”. (Harvey 2020). Kuva yritetään ladata PHP-koodin päätteellä muodossa kuva.jpg.php, että haittakoodia voidaan hyödyntää. Haittakoodi lisättiin suoraan kuvaan, koska yleinen suodatin on katsoa tiedoston sisältöä, joka on nyt suurimmaksi osaksi kuva tiedostoa eli palvelin tunnistaa tiedoston kuvana. Kun kuva on saatu ladattua verkkosovellukselle, hyökkääjän tulee seuraavaksi löytää mihin kansioon kuva on ladattu komentojen etäsuoritusta varten.



Kuva 5: Verkkosovelluspalvelin jalansija

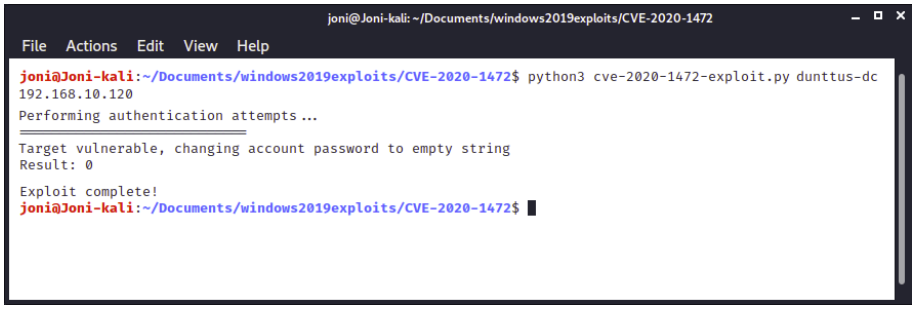
Hyödyntäminen suoraan selaimen hakupalkista kuva tiedoston PHP-funktiolla ”fun” ja Pentestmonkeyn käänteisen yhteyden Python koodia hyödyntäen. Kuvassa 5 hyödynnetään käänteisen yhteyden luovaa Python koodia, joka lähettää yhteyden Kali Linuxin sisäverkon osoitteeseen. (Pentestmonkey 2011). Terminaaliin saadaan yhteys NetCat ohjelmiston avulla kuuntelemalla sisäänpäin tulevia verkkopyyntöjä lipuilla -vnlp verkkoportista 1234 (Oracle 2017.) Apache2:lla ylläpidetyssä verkkosoveluksessa käyttäjänä toimii www-data tunnus, jota voidaan hyödyntää sisäverkon tiedustelussa.

6.2.4 Hyödyntäminen

Tunkeutumisen toinen vaihe tässä vaiheessa on tyypillistä, että hyökkääjä saavuttaa jalansijan kohde järjestelmässä. Kun hyökkääjällä on jalansija järjestelmässä, voidaan aloittaa oikeat hyökkäykset ja järjestelmän sisäinen tiedustelu. (Hutchins ym. 2010). Jos organisaatio havaitsee hyökkääjän päässeen tänne asti organisaation pitää aloittaa tietoturva poikkeus tilanteesta selviytymissuunnitelma. Tässä vaiheessa havainnollistetaan miten vakava haavoittuvuus, Windows palvelimista löytyi vuoden 2020 lopulla ja miten salasanatonta verkkotunnus ohjaimen käyttäjää voidaan hyödyntää palvelimessa, jota ei olla päivitetty.

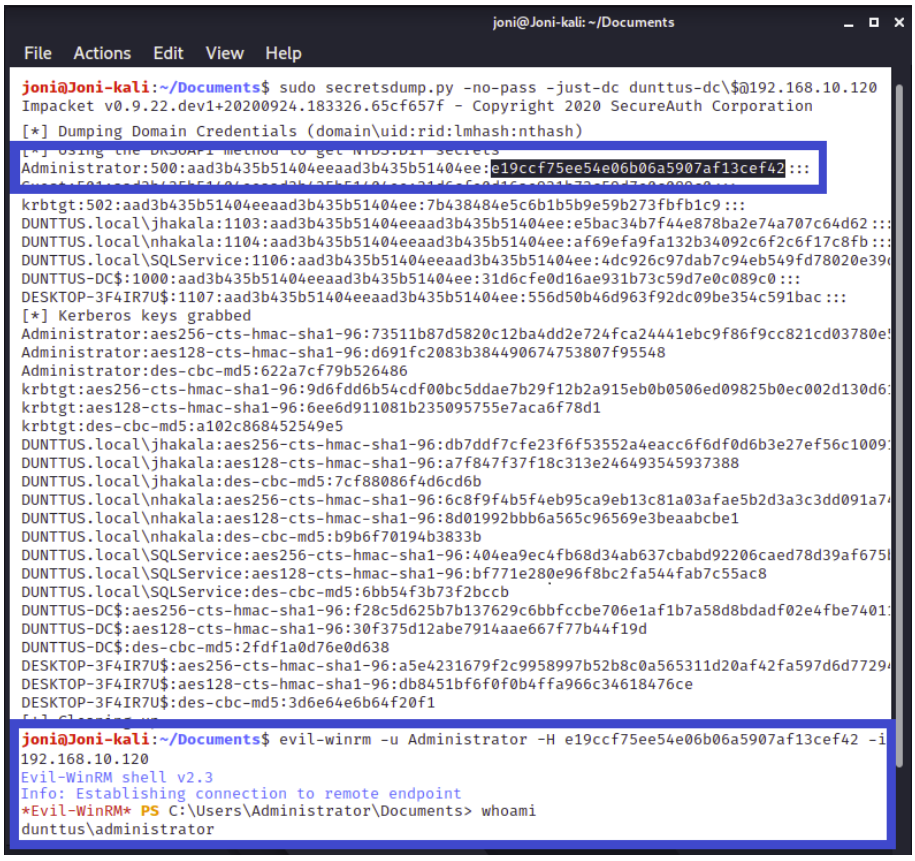
Tämän vaiheen tavoite on oikeuksien laajentaminen järjestelmässä, koska seuraavissa vaiheissa tarvitaan oikeuksia ohjelmistojen asentamiseen. Oikeuksien laajentaminen voidaan saavuttaa etsimällä haavoittuvuuksia asennetuista ohjelmistoista tai löytämällä järjestelmänvalvojan käyttäjätunnus käyttöön. Sovelluksia hyödynnetään usein oikeuksien laajennuksessa, koska niillä on enemmän käyttöoikeuksia kuin sovelluskehittäjä tai järjestelmänvalvoja on suunnitellut ja sovellukset kykenevät myös suorittamaan todella korkean tason komentoja järjestelmissä. Hyökkääjä voi saada sovelluksen oikeudet käyttöönsä saamalla sovellus ajamaan komento, joka antaa hyökkääjälle etäyhteyden sovellukselle tarkoitetuilla oikeuksilla. (Banach 2019).

Päivittämättömään Windows palvelimeen toimii Zerologon haavoittuvaisuus, mutta aktiivihakemisto palvelin näkyy vain organisaation sisäverkossa. Haavoittuvaisuudelle tarvitaan toimitustapa esim. Organisaation langattomaan verkkoon pääsy tai jostain ulkoverkkoon näkyvästä järjestelmästä jalansija, kuten edellisen kohdan verkkosovellus palvelimesta. Zerologon haavoittuvaisuus perustuu Securan löytämään konseptiin, jossa hyödynnetään Windowsin NetLogon haavoittuvuutta istunnon avaimen neuvotteluvaiheessa. Palvelinta vastaan hyökkäyksessä hyödynnetään todennusprotokollan tietoturva puutteita, jonka avulla hyökkääjä voi vaihtaa verkkotunnus ohjaimen järjestelmäkäyttäjän salasanan tyhjäksi merkkijonoksi. Zerologon haavoittuvuus oli viime vuoden vaarallisin tietoturva heikkous Windows palvelimille ja sai CVSS eli Common Vulnerability Scoring System tai suomeksi yhteinen haavoittuvuus pisteytysjärjestelmä, josta Zerologon haavoittuvuus sai pisteet 10/10 Microsoftilta. (Tervoort 2020).



Kuva 6: Zerologon hyödyntäminen

Seuraavaksi suoritettu kuvan 6 mukainen Zerologon haavoittuvuuden hyödyntäminen kohde aktiivihakemisto palvelimeen. Hyökkäys voidaan itse koodata tai ladata hyökkäyksiä jakavalta sivustoilta tässä tapauksessa tulee varmistaa lähdekoodista, ettei se suorita ei toivottua haittakoodia. Zerologon hyötykuorman toimitus tapahtuu sisäverkon yli palvelimen osoitteeseen Python ohjelmointikieltä hyödyntäen. Hyökkäyksessä on yleisesti mukana haavoittuvuuden tunnistava ominaisuus, joka kertoo hyökkäyksen onnistumisesta. Kuvan 6 mukaisesti hyökkäys onnistui palvelimeen eli verkkotunnus ohjaimen järjestelmäkäyttäjällä ei ole enää salasanaa. Jos palvelin on päivitetty tämä hyökkäys ei toimi, koska Microsoft on korjannut haavoittuvuuden tietoturvapäivitys versiossa KB4571723 11. elokuuta 2020 (Microsoft support 2020.)



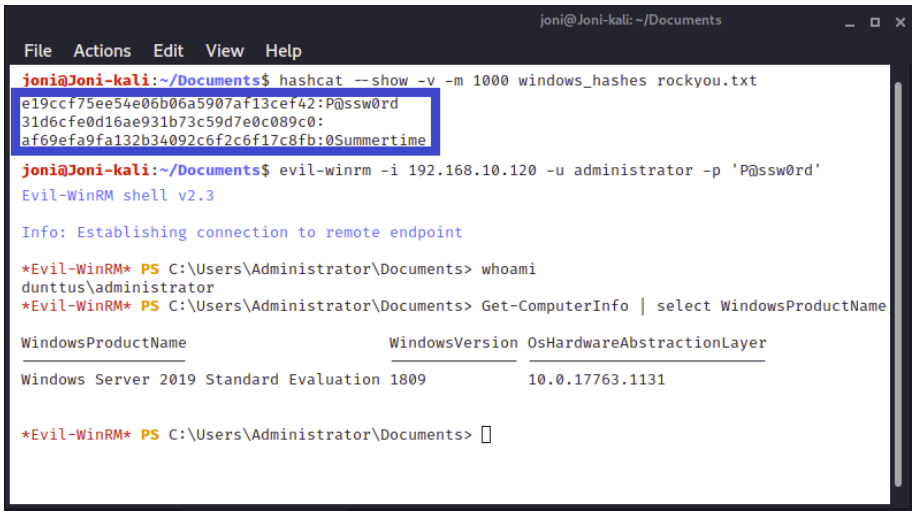
Kuva 7: DCSync ja Pass-to-Hash hyökkäys

Seuraavaksi suoritettu kuvan 7 mukainen DCSync hyökkäys, tämä hyökkäys ei voi hakea tietoja ilman toimivaa käyttäjätunnusta verkkotunnus alueelta, mutta nyt dunttus verkkotunnuksen ohjain käyttäjän salasana on tyhjä merkkijono. Voidaan siis aloittaa Zerologon haavoittuvuuden hyödyntäminen. Kuvassa 7 havainnollistettu DCSync hyökkäys löytyy Impacket ohjelmisto kirjastosta nimellä secretdump.py. Verkkotunnuksenohjain käyttäjällä voidaan hakea sisäverkon yli kaikki verkkotunnuksien käyttäjä tunnistetiedot ja salasanat salatussa muodossa. Kuvan 7 mukaisesti järjestelmästä saadaan ulostulo arvona kaikki verkkotunnus alueen käyttäjät ja salasanat salatussa muodossa.

Saaduista käyttäjätunnuksista korkeimmilla oikeuksilla toimii aktiivihakemisto palvelimen Administrator käyttäjä, jolle kuvan 7 mukaisesti kirjaudutaan Pass-to-Hash menetelmällä käyttämällä salasanaa salatussa muodossa. Pass-to-Hash ominaisuus sisältyy Evil-WinRM ohjelmistoon ja onnistuu vain kirjautuessa järjestelmään, joka käyttää samaa salausmenetelmää kuten tässä tilanteessa.

Tunkeutumisen tappoketjua käytettäessä hyökkäykseen tarvitaan ymmärrystä, että menetelmän käyttäjä tietää voidaanko jokin vaihe ohittaa. Tässä vaiheessa hyökkääjällä on käytössä aktiivihakemisto järjestelmän korkeimmilla oikeuksilla oleva tunnus eli asennus vaihetta ei välttämättä tarvita. Seuraavaksi voitaisiin siirtyä C2 tai toimet vaiheeseen.

Jos hyökkääjä saa haltuunsa salasanoja salatussa muodossa purkaminen onnistuu helposti selkokieliseksi, jos se löytyy vertailuarvo salasanalistasta. Kali Linux käyttöjärjestelmästä löytyy oletuksena rockyou.txt salasanalista, jossa on 14 341 564 yksilöllistä salasanaa, joita on käytetty 32 603 388 käyttäjätilillä (Burns 2019). Jos salasana löytyy kyseisestä listasta, salausta voidaan verrata rockyou.txt listan vertailuarvoon ja salasana saadaan selkokielisenä.



Kuva 8: Hashcat salasanan murtaminen

Windows 2019 aktiivihakemiston salasanoissa käytetään verkkotunnuksen alueen autentikoinnissa NTLM-salausta. Kuva 8 esimerkin mukaisesti Hashcat ohjelmistolle kerrotaan salauksen laatu eli NTLM, joka valitaan lipulla -m 1000. Salattuna salasanana toimii hyökkääjän löytämät Windows palvelimen NTLM-salatut salasanat ja vertailuarvona rockyou.txt salasanalista. (Hashcat 2020). Kuvan 8 mukaisesti kaksi huonoa salasanaa ”P@ssw0rd” ja ”0Summertime” murretaan selkokieliseksi. Yksi salasanoista ei löytynyt rockyou.txt salasanalistasta ja sitä ei saada murrettua tällä menetelmällä. Salasanat, jotka saadaan murrettua ovat hyökkääjän hyödynnettävissä selkokielisenä. Murrettuja salasanoja voidaan hyödyntää varsinkin, jos samaa salasanaa on käytetty useampaan järjestelmään. Kun hyökkääjä saa salasanan murrettua salauksesta sitä voidaan hyödyntää normaalisti kirjautumalla muihin järjestelmiin, jotka käyttävät eri salausta.

6.2.5 Asennus

Asennus vaiheen tarkoituksena on etäkäytön pysyvyyden ylläpitäminen. Etäyhteys tulee siis ylläpitää, jopa järjestelmän kaatumisen tai uudelleenkäynnistyksen jälkeen. Tähän vaiheeseen tarvitaan käyttäjä, jolla on oikeudet asentaa ohjelmistoja järjestelmälle. Järjestelmässä pysyvyys voidaan saavuttaa asentamalla oma takaovi järjestelmään. (Hutchins ym. 2010).

Järjestelmässä pysyvyys voidaan saavuttaa myös sivusuuntaisella liikkeellä eli hyökätään viereiseen järjestelmään ja saavutetaan jalansija myös siihen. Myöhemmin kun kohde organisaatio huomaa pääkohteen saastuneen, järjestelmä asennetaan kokonaan uudestaan ja asennettu takaovi poistuu. Tässä tapauksessa, jos hyökkääjällä on vielä viereisessä järjestelmässä takaovi ja sitä ei huomata. Hyökkäys voidaan aloittaa uudestaan suoraan organisaation sisäverkosta käsin. (Hillman & Carrington 2019).

6.2.6 C2

C2 eli englanniksi Command and control on vaihe, jonka tarkoituksena ottaa järjestelmä hyökkääjän haltuun takaoven kautta etäkomentoja lähettävällä palvelimella. C2 vaiheessa tyypillistä, että hyökkääjällä on käytössä kaikki järjestelmän toiminnot ja kykenee hyödyntämään niitä. Tämän vaiheen tavoitteena on piilottaa järjestelmään jääneitä jälkiä hyökkäyksestä ja tehdä takaovi yhteydestä vaikeasti löydettävä ohjelmisto. Kokonaisuudessaan tämän vaiheen tarkoitus on minimoida riskiä jäädä kiinni ja ylläpitää yhteys saastuneeseen palvelimeen, koska jos järjestelmän puolustava taho huomaa hyökkäyksen palvelin uudelleen asennetaan ja haavoittuvuudet korjataan. (Hutchins ym. 2010).

Takaovi voidaan piilottaa normaali Windows prosessien joukkoon ja käyttää sitä vain normaali työaikoina, että se sulautuu normaaliin verkkoliikenteeseen. Yhteyden ei myöskään

kannata olla pitkään jatkuvaa, koska tämä on helposti huomattavissa. Saastuneen palvelimen tulee lähettää signaali takaisin hyökkäävälle palvelimelle, kun kohteeseen tarvitaan uusi etäyhteys. (Hutchins ym. 2010).

6.2.7 Toimet

Tässä vaiheessa suoritetaan toimet, jonka takia hyökkäys on alun perin aloitettu. Toimet riippuvat siitä mitä palvelimella voidaan tehdä, mitä tietoja palvelin sisältää ja tuleeko palvelimelle jotain tärkeitä tietoja. Palvelimen ominaisuuksia voidaan tiedustella ja niiden perusteella tehdä erilaisia toimintoja, joita voi olla aktiivinen vakoilu, tietojen varastaminen, tietojen salaaminen ja organisaation kiristys. (Hutchins ym. 2010).

Häijy hyökkääjä voi käyttää kiristysohjelman laukaisussa myyntitekniikoita, kuten kiireellisen hätätilanteen luominen. Kiristysohjelman parasta ajankohtaa voidaan tutkia suoraan organisaation julkisen sosiaalisen media sivuston kautta ja etsiä organisaatiolle tärkeitä ajankohtia. Ohjelma voidaan laukaista, vaikka tuntia ennen yritykselle tärkeää tapahtumaa ja luoda yritykselle kiireellinen hätätilanne maksaa lunnaita. (Cimpanu 2021). Lunnaita ei tietenkään kannata koskaan maksaa, koska hyökkääjään ei kannata luottaa ja lunnaiden maksaminen tukee hyökkääjien toimintaa. Organisaatio voi tässä vaiheessa tuoda tiedot takaisin varmuuskopiosta, jos ne on tehty oikein.

7 Onko palvelimeen murtauduttu

Murtautuminen on hyvä huomata mahdollisimman nopeasti, koska hyökkääjä voi peittää murtautumisen jälkiä, jos saa tarpeeksi oikeuksia järjestelmässä. Hyökkäyksien jälkiä voidaan peittää todella tehokkaasti poistamalla lokitietoja hyökkäyksestä ja piilottamalla takaovi järjestelmän luotettuun ohjelmaan. Jos murtautumista ei huomata ollenkaan hyökkääjä voi jäädä järjestelmään vakoilemaan pitkäksikin aikaa. Rikollisryhmien hyökkäyksien tarkoituksena maksimoida omat taloudelliset hyödyt. Hyökkääjät voivat yrittää laajentaa hyökkäystä saastuttamalla pahimmassa tapauksessa varmuuskopiot, yrityksen asiakkaiden järjestelmät ja yhteistyökumppaneiden järjestelmät.

Esimerkkinä yrityksen asiakkaiden järjestelmien saastuttamisesta vuoden 2020 lopulla tapahtui laajin kyberhyökkäys, joka on koskaan tapahtunut. Tämän hyökkäyksen levityksessä hyödynnettiin luotetun ohjelmistoyritys SolarWindsin Orion ohjelmiston päivityksiin piilotettua DLL-tiedostoa, joka avasi hyökkääjille takaoven asiakkaiden järjestelmiin (Microsoft 2021.) SolarWinds asiakkaita, joihin hyökkäys vaikutti, oli todella suuria yrityksiä kuten Cisco, Intel, Nvidia, Belkin, and VMware (Clark 2020.) Hyökkäyksen laajuuden takia kaikkia hyökkäyksen vaikutuksia ei ole edes vielä tiedossa, kuten mitä tietoja hyökkääjät ovat keränneet ja mihin tietoja tullaan hyödyntämään.

Palvelimelta voi itse etsiä tunkeutumisen merkkejä, mutta tämä on niin laaja alue, ettei tässä tutkielmassa paneuduta tähän muuten kuin pintaraapaisun verran. Palvelinta voidaan tutkia havaitsemalla poikkeavuus tilanteet normaalista tilanteesta. Useasti tietoturvallisuus ohjelmistot tekevät näitä toimintoja automaattisesti. Palvelimelta voidaan tarkistaa tietokoneen käynnistyksen yhteydessä ajavat oudot ohjelmistot ja mitä ne tekevät. Muusta verkkoliikenteestä poikkeavat yhteydet tai verkko osoitteet voidaan tarkastaa luotetuksi. Koko järjestelmän tiedostojen muokkaus ajat voidaan tarkastaa ja miksi jokin tiedosto on muokattu johonkin outoon aikaan. Hyvä myös tarkistaa käykö jokin käyttäjätunnus outoihin aikoihin tekemässä toimintoja organisaation järjestelmässä. Järjestelmään kerättyjä vanhoja lokitietoja voidaan tulkita ja poimia mahdollisesti outoja merkintöjä tarkastukseen. Jälkikäteen voi olla vaikea tutkia hyökkäystä, jos tapahtumasta ei kerätä lokeja tai jos hyökkääjä on saanut lokitiedot omaan hallintaansa. (Murphy 2020).

8 Pohdinta

Tutkielman tarkoituksena oli parantaa aktiivihakemisto palvelimen tietoturvaa selvittämällä parhaita käytäntöjä ja menetelmiä aktiivihakemisto palvelimen tietoturvaan katsottuna. Tutkimuksen menetelmän tarkoituksena tarkastella kriittisesti parhaita käytäntöjä ja kokeilemalla vahvistaa miksi niitä tarvitaan. Tutkielman tarkoituksena ei ole antaa kuvaa, että kriittiset tietoturva virheet aktiivihakemistossa olisivat todella yleisiä vain näyttää miten ne toimivat oikeassa tilanteessa.

Tutkimuskysymyksiin vastauksia lyhyesti:

1. Miksi Active Directoryn tietoturva on tärkeää?
   Aktiivihakemistoa hyödyntää suurin osa yrityksistä eli se on isossa osassa yrityksien tietoturvaa. Aktiivihakemisto palvelin on yrityksen tärkein palvelin tietoturvaan katsottuna, koska sillä on paljon valtaa yrityksen sisäverkossa. Aktiivihakemisto palvelimen kautta voidaan esimerkiksi levittää haittaohjelmia kaikkiin yrityksen tietokoneisiin, jotka käyttävät verkkonimi aluetta.

2. Mitä ovat Windows palvelimien parhaat käytännöt?
   Windows palvelimen kokoonpanoasetukset tulee tehdä harkitusti, koska jotkin asetukset ovat tarkoitettu erityistilanteisiin ja laittamalla niitä päälle voidaan luoda lisää hyökkäyspinta-alaa. Loppukäyttäjät ovat isossa osassa aktiivihakemisto Windows palvelimen tietoturvaa, koska hyökkääjä voi saada jalansijan sisäverkon järjestelmiin loppukäyttäjän tunnuksesta ja hyödyntää yrityksen käyttäjätunnuksien oikeuksia. Käyttäjien suurin vastuu on pitää oma käyttäjätunnus vain omassa käytössään eli käyttäjien tulee käyttää vain vahvoja järjestelmälle uniikkeja salasanoja.

3. Miten parantaa Windows palvelimen tietoturvaa?
   Windows palvelimen tietoturvaa voidaan parantaa aktiivisen puolustamisen menetelmillä ja noudattamalla parhaita käytäntöjä. Aktiivisen puolustuksen menetelmiä on lukuisia, mutta tässä tutkimuksessa keskityttiin OODA-silmukka menetelmään, CIA-kolmio malliin, riskienhallintaan, Intrusion Kill Chain menetelmään ja mahdollisiin hyökkäyksiin. Kaikki nämä aktiivisen puolustuksen menetelmät tukevat Windows palvelimen tietoturvaa.

Windows palvelimet ovat melko tietoturvallisia oikein käytettyinä ja parhaat käytännöt ei ole turhia vaan estää suurimman osan hyökkäyksistä. Aktiivihakemistoon kohdistuvat tietoturvariskit tulee yleisesti käyttäjien tai ylläpidon huonosta toiminnasta. Pienillä tietoturvakäytäntöjen korjauksilla, kuten salasanojen vahvana pitämisellä ja järjestelmän päivityksillä on iso vaikutus tietoturvan kokonaiskuvaan katsottuna. Yleinen tietoturvaa kuvaava sanonta tietoturvasi on yhtä vahva kuin järjestelmäsi heikoin lenkki sopii hyvin aktiivihakemisto palvelimeen, koska käyttäjistä saadaan helposti jalansija sisäverkon järjestelmiin. Aktiivinen viimeisimpien tietoturvauutisten seuraaminen on hyvä tapa tehdä päätöksiä esim. Järjestelmän päivityksien kannalta ja lisäosien mahdollisesta väliaikaisesta sulkemisesta tai poistamisesta. Hyökkäyksiä on myös melko helppo toteuttaa ilman mitään en-

nakkotietoa hyökkäyksien tekemisestä, mutta aktiivisen puolustamisen menetelmät ja parhaat käytännöt torjuisivat kaikki hyökkäykset, joita tämän tutkielman hyökkäysvaiheessa suoritetaan.

Tiedon tietoturvallinen säilytys on yksi tärkeimmistä tietoturvan tehtävistä. Asiakas tietojen menetys voi johtaa yrityksen hyvän maineen menetykseen asiakkaiden näkökulmasta. Pienikin määrä tietoa väärissä käsissä on väärin käytettävissä esim. Kohdennetussa kalastelu sähköposteissa. Usein vuotanut tieto ei myöskään vanhene, sillä kuinka usein ihmiset vaihtavat puhelinnumeroa, osoitetta tai henkilötunnusta? Organisaation tietoturvaa suunniteltaessa kannattaa pitää mielessä Warren Buffettin sanonta:

> *"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."* (Buffett, W 2012).

Varonisen tekemän kyselyn vastauksien perusteella 64 prosenttia amerikkalaisista ei ole ikinä katsonut onko tunnukset vuotanut julkisuuteen, kyselyyn oli vastannut yli 1000 henkilöä (Sobers 2019.) Käyttäjiä kannattaa omasta mielestäni ohjata myös tarkastamaan onko salasanat vuotaneet julkiseen verkkoon, koska tämä voi toimia herätteenä uusimaan omaa salasanaa.

Lockheed Martinin Intrusion Kill Chain on jo vähän vanhentunut malli, koska joitain vaiheita voidaan ohittaa. Alkuperäisessä vuonna 2010 tehdyssä ohjeistuksessa hyökkäys voidaan katkaista estämällä hyökkäys missä tahansa ketjun vaiheessa. Hyökkäyksiä kokeilemalla voidaan todeta, että ainakaan nykypäivän hyökkäyksissä tämä ei ole totta. Hyökkääjä voi löytää kohteen tiedustelu vaiheessa järjestelmästä haavoittuvuuden, joka mahdollistaa järjestelmän korkeimmat oikeudet. Suurilla oikeuksilla voidaan hypätä toimitusvaiheesta suoraan toimintoihin eli kokonaisen organisaation tietojen varastamiseen ja kiristys ohjelmiston asentamiseen. Tunkeutumisen tappoketju soveltuu omasta mielestäni paremmin jo tapahtuneen hyökkäyksen tutkimiseen tai hyökkäyksien demonstroitiin, kuin hyökkäyksien estämiseen.

Opin tutkimusta kirjoittaessa todella paljon aktiivihakemiston tietoturvasta, parhaista käytännöistä ja tietoturvan menetelmistä. Yllättävinä tilanteina tutkimuksen aikana kokeilin omaan vanhaan Windows Server 2019 palvelimeen Zerologon haavoittuvuutta ja se toimi kyseiseen palvelimeen. Toinen yllättävä tilanne tutkimusmenetelmän aikana, kun latasin verkkoon vuotaneen käyttäjätunnus/salasana listan. Listasta löysin omia vanhoja tunnuksia ja salasanoja selkokielisenä. Koen päässeeni tutkielman alkuperäiseen tavoitteeseen aktiivihakemisto palvelimen tietoturvan parantamisessa. Toivottavasti oppinäytetyöstäni on myös hyötyä jollekin aktiivihakemistoa käyttävälle taholle tietoturvan parantamisessa.

Lähteet

Abbott, J. & Garcia, V. 2015. Password differences based on language and testing of memory recall. Luettavissa: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.681.5392&rep=rep1&type=pdf. Luettu: 2.4.2021

Al-Ansary, H. 2014. Modern Education and Computer Science. Luettavissa: https://www.researchgate.net/publication/343650398_Modern_Education_and_Computer_Science. Luettu: 15.4.2021

Banach, Z. 2019. What Is Privilege Escalation and Why Is It Important?. Luettavissa: https://www.netsparker.com/blog/web-security/privilege-escalation/. Luettu: 27.4.2021

BeyondTrust 2020. Pass-the-Hash (PtH) Attack. Luettavissa: https://www.beyondtrust.com/resources/glossary/pass-the-hash-pth-attack. Luettu: 21.4.2021

Brehmer, B. 2005. The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control. Luettavissa: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.489.817&rep=rep1&type=pdf. Luettu: 20.4.2021

Burns, W. 2019. Common Password List (rockyou.txt). Luettavissa: https://www.kaggle.com/wjburns/common-password-list-rockyoutxt. Luettu: 4.4.2021

Buffett, W. 2012. Quotable Quote. Luettavissa: https://www.goodreads.com/quotes/618606-it-takes-20-years-to-build-a-reputation-and-five. Luettu: 29.4.2021

Cimpanu, C. 2021. Ransomware gang tries to extort Apple hours ahead of Spring Loaded event. Luettavissa: https://therecord.media/ransomware-gang-tries-to-extort-apple-hours-ahead-of-spring-loaded-event/. Luettu: 29.4.2021

CIS Benchmarks 2020. CIS Microsoft Windows Server 2019 RTM (Release 1809) Benchmark. Luettavissa: https://www.cisecurity.org/benchmark/microsoft_windows_server/. Luettu: 29.3.2021

Clark, M. 2020. Big tech companies including Intel, Nvidia, and Cisco were all infected during the SolarWinds hack. Luettavissa: https://www.theverge.com/2020/12/21/22194183/intel-nvidia-cisco-government-infected-solarwinds-hack. Luettu: 29.4.2021

Debbie Walkowski 2019. What Is the CIA Triad? Luettavissa: https://www.f5.com/labs/articles/education/what-is-the-cia-triad. Luettu: 20.4.2021

die.net 2011. nmap(1) - Linux man page. Luettavissa: https://linux.die.net/man/1/nmap. Luettu: 20.3.2021

DNSstuff 2019. The Ultimate Guide to Active Directory Best Practices. Luettavissa: https://www.dnsstuff.com/active-directory-best-practices. Luettu 1.4.2021

FarnamStreet 2021. The OODA Loop: How Fighter Pilots Make Fast and Accurate Decisions. Luettavissa: https://fs.blog/2021/03/ooda-loop/. Luettu: 5.4.2021

Finlex 2015. Tieto- ja viestintärikoksista. Luettavissa: https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L38. Luettu: 3.4.2021

Goel, J. & Mehtre, B. 2015. Vulnerability assessment & penetration testing as a cyber defence technology. Luettavissa: https://www.sciencedirect.com/science/article/pii/S1877050915019870/. Luettu: 21.4.2021

Haaga-Helia 2014. Haaga-Helian IT-palvelujen käyttösäännöt. Luettavissa: https://www.haaga-helia.fi/fi/haaga-helian-it-palvelujen-kayttosaannot. Luettu: 2.4.2021

Harvey, P. 2020. exiftool Application Documentation. Luettavissa: https://exiftool.org/exiftool_pod.html. Luettu: 27.4.2021

Hashcat 2020. hashcat. Luettavissa: https://hashcat.net/wiki/doku.php?id=hashcat. Luettu: 27.4.2021

Hillman, M. & Carrington, T. 2019. AutoCAD - Designing a Kill Chain. Luettavissa: https://labs.f-secure.com/blog/autocad-designing-a-kill-chain/. Luettu: 27.4.2021

Hutchins, E., Cloppert, M. & Amin, R. 2010. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Luettavissa: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf. Luettu: 22.4.2021

Krishnamoorthi, S., Carleton, J. 2020. Active Directory Holds the Keys to your Kingdom, but is it Secure? Luettavissa: https://images.discover.frost.com/Web/FrostSullivan/%7B6198df00-ed17-4d0d-bae8-e47a74339398%7D_FS_WP_Alsid-AD_14Feb20-v2_jw.pdf. Luettu: 27.3.2021

Lockheed Martin Corporation 2015. Seven Ways to Apply the Cyber Kill Chain® with a Threat Intelligence Platform. Luettavissa: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf. Luettu: 22.4.2021

Lystrup, O. 2016. Cisco Security Report: Majority of Orgs Do Not Monitor DNS. Luettavissa: https://umbrella.cisco.com/blog/cisco-security-report-more-orgs-should-be-monitoring-dns. Luettu: 30.3.2021

Microsoft 2009. Active Directory Architecture. Luettavissa: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb727030(v=technet.10). Luettu: 22.4.2021

Microsoft 2016. Mitigating Pass-the-Hash and Other Credential Theft, version 2. Luettavissa: https://docs.microsoft.com/en-us/previous-versions/dn785092(v=msdn.10). Luettu: 21.4.2021

Microsoft 2017. Active Directory Domain Services Overview. Luettavissa: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview. Luettu:20.4.2021

Microsoft 2019. Active Directory on-Demand -arvioinnin käytön aloittaminen. Luettavissa: https://docs.microsoft.com/fi-fi/services-hub/unified/health/getting-started-ad. Luettu: 18.4.2021

Microsoft 2020. Microsoft Digital Defense Report September 2020. Luettavissa: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWxPuf. Luettu: 31.3.2021

Microsoft 2021. Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop. Luettavissa: https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/. Luettu: 29.4.2021

Microsoft support 2020. How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472. Luettavissa: https://support.microsoft.com/kb/4557222. Luettu: 20.4.2021

Murphy, D. 2020. Top 10 Signs That Your System Has Been Compromised. Luettavissa: https://www.lepide.com/blog/top-10-signs-that-your-system-has-been-compromised/. Luettu: 29.4.2021

National Cyber Security Centre 2018. Spray you, spray me: defending against password spraying attacks. Luettavissa: https://www.ncsc.gov.uk/blog-post/spray-you-spray-me-defending-against-password-spraying-attacks. Luettu 1.4.2021

Oracle 2017. netcat(1). Luettavissa: https://docs.oracle.com/cd/E86824_01/html/E54763/netcat-1.html. Luettu: 6.5.2021

Pentestmonkey 2011. Reverse Shell Cheat Sheet. Luettavissa: http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet. Luettu: 25.4.2021

Perelman 2014. Security. Luettavissa: https://www.med.upenn.edu/pmacs/user-responsibilities.html. Luettu: 2.4.2021

Petters, J. 2020. IDS vs. IPS: What is the Difference? Luettavissa: https://www.varonis.com/blog/ids-vs-ips/. Luettu: 12.4.2021

Poston, H. 2020. What are Black Box, Grey Box, and White Box Penetration Testing? [Updated 2020]. Luettavissa: https://resources.infosecinstitute.com/topic/what-are-black-box-grey-box-and-white-box-penetration-testing/. Luettu: 3.4.2021

Reiner, D., Press, G., Lenaghan, M. & Barta, D. 2004. Information Lifecycle Management: The EMC Perspective. Luettavissa: https://www.academia.edu/download/50698799/ICDE.2004.132005220161203-25953-1tmskte.pdf. Luettu: 7.4.2021

Rieger, T. 2021. Vulnerabilities to Cognitive Biases in the OODA Loop Process. Luettavissa: https://nsiteam.com/social/wp-content/uploads/2021/01/Invited-Perspective_OODA-Loop_FINAL.pdf. Luettu: 1.4.2021

Ross, E., McIllece, J. & Gerend, J. 2020. Domain Name System (DNS). Luettavissa: https://docs.microsoft.com/en-us/windows-server/networking/dns/dns-top. Luettu: 29.3.2020

Sławińska, S. 2020. Cyber Kill Chain – what is it and how to use it to stop advanced methods of attack? Luettavissa: https://seqred.pl/en/cyber-kill-chain-what-is-it-and-how-to-use-it-to-stop-advanced-methods-of-attack/. Luettu: 27.3.2021

Sobers, R. 2019. 64% of Americans Don’t Know What to Do After a Data Breach — Do You? (Survey). Luettavissa: https://www.varonis.com/blog/data-breach-literacy-survey/. Luettu: 30.4.2021

Stealthbits Technologies 2021. LDAP Reconnaissance. Luettavissa: https://attack.stealthbits.com/ldap-reconnaissance-active-directory. Luettu: 20.4.2021

Stewart, J., Chapple, M. & Gibson, D. 2012. Certified Information Systems Security Professional Study Guide, 6th Edition. Sybex/Wiley California.

Tervoort, T. 2020. WHITEPAPER Zerologon: Unauthenticated domain controller compromise by subverting Netlogon cryptography (CVE-2020-1472). Luettavissa: https://www.secura.com/uploads/whitepapers/Zerologon.pdf. Luettu: 25.4.2021

Traficom Kyberturvallisuuskeskus 2019. Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Office%20365%20opas%20aukeamat.pdf. Luettu: 7.4.2021

Traficom Kyberturvallisuuskeskus 2020. Kriittisen Zerologon -haavoittuvuuden aktiivinen hyväksikäyttö on alkanut. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kriittisen-zerologon-haavoittuvuuden-aktiivinen-hyvaksikaytto-alkanut. Luettu: 28.4.2021

Tyson, J. 2019. The CIA Triad. Luettavissa: https://blog.jamestyson.co.uk/the-cia-and-dad-triads. Luettu: 7.4.2021

Valtiovarainministeriö 2017. Ohje riskienhallintaan. Luettavissa: https://www.suomidigi.fi/sites/default/files/2020-06/VM_22_2017_1.pdf. Luettu 15.4.2021

Valtiovarainministeriö 2017. Tietoturvapoikkeamatilanteidenhallinta. Luettavissa: https://www.suomidigi.fi/sites/default/files/2020-06/VM_8_2017.pdf. Luettu: 15.4.2021

Van Cott, J. 2020. What are DCSync and DCShadow Active Directory attacks? Luettavissa: https://www.lepide.com/blog/what-are-dcsync-and-dcshadow-active-directory-attacks/. Luettu: 20.4.2021

Verizon 2020. Data Breach Investigations Report Luettavissa: https://enterprise.verizon.com/resources/reports/dbir/. Luettu: 17.4.2021

VisualParadigm 2021. What is OODA Loop? Luettavissa: https://online.visual-paradigm.com/knowledge/decision-analysis/what-is-ooda-loop/. Luettu: 5.4.2021

Vogel, M. 2019. Is Cybercrime a Cat and Mouse Game?. Luettavissa: https://www.zoginc.com/cybercrime-a-cat-and-mouse-game/. Luettu: 21.4.2021

Liitteet

Liite 1. Nmap porttiskannaus

joni@Joni-kali:~$ sudo nmap -sV -sC 192.168.10.120

Starting Nmap 7.91 (https://nmap.org) at 2021-03-20 00:09 EET

Nmap scan report for 192.168.10.120

Host is up (0.00038s latency).

Not shown: 988 filtered ports

PORT STATE SERVICE VERSION

53/tcp open domain Simple DNS Plus

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2021-03-19 22:09:50Z)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: DUNTTUS.local0., Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=DUNTTUS-DC.DUNTTUS.local

| Subject Alternative Name: othername:<unsupported>, DNS:DUNTTUS-DC.DUNTTUS.local

| Not valid before: 2020-06-02T19:45:49

|_Not valid after: 2021-06-02T19:45:49

|_ssl-date: 2021-03-19T22:11:09+00:00; 0s from scanner time.

445/tcp open microsoft-ds?

464/tcp open kpasswd5?

593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

636/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Domain: DUNTTUS.local0., Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=DUNTTUS-DC.DUNTTUS.local

| Subject Alternative Name: othername:<unsupported>, DNS:DUNTTUS-DC.DUNTTUS.local

| Not valid before: 2020-06-02T19:45:49

|_Not valid after: 2021-06-02T19:45:49

|_ssl-date: 2021-03-19T22:11:09+00:00; 0s from scanner time.

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: DUNTTUS.local0., Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=DUNTTUS-DC.DUNTTUS.local

| Subject Alternative Name: othername:<unsupported>, DNS:DUNTTUS-DC.DUNTTUS.local

| Not valid before: 2020-06-02T19:45:49

|_Not valid after: 2021-06-02T19:45:49

|_ssl-date: 2021-03-19T22:11:09+00:00; 0s from scanner time.

3269/tcp open ssl/ldap   Microsoft Windows Active Directory LDAP (Domain: DUNTTUS.local0., Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=DUNTTUS-DC.DUNTTUS.local

| Subject Alternative Name: othername:<unsupported>, DNS:DUNTTUS-DC.DUNTTUS.local

| Not valid before: 2020-06-02T19:45:49

|_Not valid after: 2021-06-02T19:45:49

|_ssl-date: 2021-03-19T22:11:09+00:00; 0s from scanner time.

5357/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Service Unavailable

MAC Address: DA:5E:40:F8:79:8B (Unknown)

Service Info: Host: DUNTTUS-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_nbstat: NetBIOS name: DUNTTUS-DC, NetBIOS user: <unknown>, NetBIOS MAC: da:5e:40:f8:79:8b (unknown)

| smb2-security-mode:

| 2.02:

|_ Message signing enabled and required

| smb2-time:

| date: 2021-03-19T22:10:29

|_ start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 90.22 seconds