



SAVONIA

OPINNÄYTETYÖ - AMMATTIKORKEAKOULUTUTKINTO
TEKNIIKAN JA LIIKENTEEN ALA

AKTIIVIHAKEMISTON DO- KUMENTOINTI

TEKIJÄ/T:

Piibe Tori

| | |
|---|--------------------------|
| Koulutusala Tekniikan ja liikenteen ala | |
| Tutkinto-ohjelma Tietotekniikan tutkinto-ohjelma | |
| Työn tekijä(t) Piibe Tori | |
| Työn nimi Aktiivihakemiston dokumentaatio | |
| Päiväys 22.12.2020 | Sivumäärä/Liitteet 28 |
| Toimeksiantaja/Yhteistyökumppani(t) Valtion tieto- ja viestintätekniikkakeskus Valtori | |
| <p>Tiivistelmä</p> <p>Tässä opinnäytetyössä kuvattiin ensimmäisessä osiossa, miksi aktiivihakemistoa kannattaa dokumentoida. Toisessa osiossa tuotettiin aktiivihakemiston dokumentaatiotyökalu. Aktiivihakemisto toimii keski- ja suurikokoisten yritysten selkärankana. Siksi on tärkeää, että yrityksen IT-ylläpitäjillä on selkeä kuva sen ympäristöstä ja asetuksista. Dokumentaation tärkeys korostuu tänä päivänä selkeästi myös tietoturva-asetusten noudattamisessa.</p> <p>Aktiivihakemiston dokumentoinnilla voidaan saavuttaa monia tärkeitä ominaisuuksia ja etuja. Sillä voidaan helpottaa vianselvitystä ja järjestelmän palautumista vikatiloista, yhtenäisempää kuvaa järjestelmästä ja sen tietoturvasta ja helpottamaan tiedonsiirtoa ylläpitäjien vaihtuessa.</p> <p>Työn tutkimusosiossa hyödynnettiin eri alojen asiantuntijoiden ammattitaitoa. Dokumentaatiotyökalun kehityksessä hyödynnettiin PowerShellia, jolla yllä mainitut osiot dokumentoitiin. Sovelluksen testausta varten rakennettiin testiympäristö Microsoft Azure-pilviympäristöön.</p> <p>Työn tuloksena syntyi toimiva PowerShell-moduuli, jolla voidaan automatisoida aktiivihakemiston dokumentaatiota. Työkalu on suunnattu alan asiantuntijoiden käytettäväksi. Moduuli käynnistetään komentokehoitteelta ja haettu tieto tallennetaan haluttuun kansioon. Jatkotoimeenpiteenä hyödynnetään koodia opinnäytetyön tekijän työnantajan ICT-ympäristössä.</p> | |
| Avainsanat Aktiivihakemisto, ICT-infrastruktuuri, dokumentaatio, tietoturva | |

| | |
|---|------------------------|
| Field of Study Technology, Communication and Transport | |
| Degree Programme Degree Programme in Information Technology | |
| Author(s) Piibe Tori | |
| Title of Thesis Documenting Active Directory | |
| Date 22.12.2020 | Pages/Appendices 28 |
| Client Organization /Partners Valtori Oy | |
| <p>Abstract</p> <p>The objective of this bachelor's thesis to research the importance of documenting Active Directory, and then to implement the knowledge by building a toolset for automating the documentation process.</p> <p>In the research section of the thesis, basic cyber threats against Active Directory were explained. By understanding common threats, it is possible to generate documentation that indicates possible threats to the system. In the theoretical part of the thesis blogs and research papers of field-experts were used. The toolset was built in PowerShell scripting framework and developed using Azure Cloud services.</p> <p>The outcome of the project was a script-toolset for automating the documentation process mentioned above.</p> | |
| Keywords Active Directory, ICT- infrastructure | |

SISÄLTÖ

| | | |
|-------|---|----|
| 1 | JOHDANTO | 6 |
| 1.1 | Työn tausta | 6 |
| 1.2 | Työn toteutus ja sen rakenne..... | 6 |
| 1.3 | Aihe ja tavoite | 6 |
| 1.4 | Käsitteet..... | 7 |
| 2 | AKTIIVIAKEMISTO JA TIETOTURVA..... | 7 |
| 2.1 | Aktiivihakemiston tietoturva | 9 |
| 2.2 | Aktiivihakemiston palautus ja testaamisen ongelmat..... | 11 |
| 2.3 | Yleisimmät hyökkäykset aktiivihakemistoa vastaan | 12 |
| 2.3.1 | Hyökkäyksen ensikontakti | 13 |
| 2.3.2 | Sisäverkossa eteneminen | 14 |
| 2.3.3 | Hyökkäyksen vahingot ja sen motiivit..... | 16 |
| 2.4 | Yleisimmät suojautumismekanismit | 16 |
| 3 | DOKUMENTAATIO | 19 |
| 3.1 | Puutteellisen dokumentaation vaikutus | 19 |
| 3.2 | Dokumentoinnin rakentaminen..... | 20 |
| 4 | TYÖN SUUNNITTELU | 20 |
| 4.1 | Työn minimivaatimukset ja rajausta | 20 |
| 4.2 | Aikataulu ja projektin kulku..... | 21 |
| 4.3 | PowerShell-moduuli..... | 21 |
| 4.4 | Kehitysympäristö..... | 21 |
| 5 | TYÖN TOTEUTUS | 21 |
| 5.1 | Kehitysympäristön alustaminen ja ohjelmakoodin hallinnointi | 22 |
| 5.2 | Tiedon keruu | 22 |
| 5.3 | Dokumentoitava data | 23 |
| 5.3.1 | Domain Controller tiedot..... | 23 |
| 5.3.2 | DNS-tiedot..... | 24 |
| 5.3.3 | Aktiivihakemisto ja tietoturva | 25 |
| 6 | YHTEENVETO JA SAAVUTETUT OMINAISUUDET | 26 |
| 6.1 | Jatkokehitys | 26 |
| | LÄHTEET | 27 |

1 JOHDANTO

Tässä toiminnallisessa opinnäytetyössä kehitettiin skriptimoduuli, joka generoi dokumentaatiotiedoston aktiivihakemistosta sekä muista ICT-ympäristön komponenteista kuten domain controller ja DNS. Skriptaustekniikkana käytettiin Powershellia, joka on Microsoftin sovellusrajapinta Windows-palvelinten ylläpitoon.

1.1 Työn tausta

Tarve opinnäytetyön aiheelle syntyi opinnäytetyöntekijän työpaikkaorganisaatiossa, missä syntyi tarve kehittää työkalu aktiivihakemistoon ja siihen liittyvien komponenttien dokumentointiin.

Aktiivihakemisto toimii keskisuurten ja suuryritysten selkärankana. Organisaation muut sovellukset ja elintärkeät toiminnot kuten työasemalle ja sähköpostiin kirjautuminen ovat riippuvaisia aktiivihakemistosta. Pahantahtoiselle hyökkääjälle aktiivihakemistoon pääsy on näköalapaikka koko organisaatioon, siksi on tärkeitä, että ylläpitäjillä on selkeä kuva palvelun tilasta ja tietoturva-asetuksista.

Työkalua on tarkoitus käyttää alan asiantuntijoiden sekä opinnäytetyöntekijän omassa organisaatiossa. Työkalu tulostaa haetun datan ulos HTML-muodossa, jota on helppoa käsitellä eri työkaluissa kuten PowerBI:ssa ja Excel:ssä. Skriptimoduulissa on hyödynnetty eri alan asiantuntijoiden parhaiksi todettuja käytäntöjä sekä skriptin mallipohjia.

Opinnäytetyö tehtiin pääosin syksyn 2020 aikana. Jatkokehitys kuitenkin jatkuu toimeksiantajan organisaatiossa.

Opinnäytetyön merkitys on myös kehittää opinnäytetyöntekijän ymmärrystä aktiivihakemiston tietoturvasta ja sen komponenteista. Opinnäytetyöntekijältä löytyy jonkin verran osaamista PowerShell-skriptauksesta, mutta opinnäytetyösään syvennyttiin aiheeseen paremmin.

1.2 Työn toteutus ja sen rakenne

Opinnäytetyön alussa tutkitaan aktiivihakemisto ja sen muita komponentteja tietoturvan kannalta. Tutkimusosion perusteella voidaan rajata dokumentoitavat aihealueet ja niiden merkitys kokonaisdokumentaatioissa. Dokumentoitavia osa-alueita käsitellään luvussa viisi.

Dokumentaatio työkalun suunnittelua ja kehitystä kuvataan luvussa neljä ja viisi. Opinnäytetyössä kuvataan myös alan asiantuntijoiden parhaita käytäntöjä PowerShell-moduulin rakentamisessa.

1.3 Aihe ja tavoite

Aktiivihakemisto toimii monien organisaatioiden ICT-ympäristöjen selkäranka. Siksi on tärkeitä varmistaa palvelunlaatua dokumentoimalla ja kehittämällä ylläpitäjien yleisymmärrystä aktiivihakemistoon liittyvistä uhista.

Opinnäytetyöllä on kaksi tavoitetta. Ensin tutkitaan aktiivihakemistoa tietoturvan kannalta ja määrittää dokumentoitavat osa-alueet. Tutkimuksen jälkeen kehitetään dokumentointiin soveltuva työkalu, jota voidaan jatkossa hyödyntää työnantaja organisaation käytössä.

Tutkimusosiossa tutkitaan aktiivihakemiston hyökkäysrajapintaa. Selvityksestä selviää, mitä asetuksia kannattaa ottaa huomioon dokumentaatioissa. Parhaita käytäntöjä seuraamalla voidaan vähentää tietoturvariskejä ICT-ympäristössä.

Aktiivihakemiston dokumentaatio on tärkeää sekä ylläpidon että mahdollisten tietoturvapoikkeamien löytämisen kannalta.

Dokumentoimalla aktiivihakemistoa voidaan:

- Helpottaa vianselvitystä ja palautuksia mahdollisissa vikatilanteissa
- Löytää mahdollisia implisiittisiä asetuksia
- Saada parempaa yleiskuva palveluntilasta
- Helpottaa tiedonsiirtoa ylläpitäjien vaihtuessa
- Tarkistaa tietoturva-asetuksia

Opinnäytetyön toiminnallisen työn tarkoituksena on toteuttaa helppokäyttöinen PowerShell-moduuli, jolla pystytään dokumentoimaan erilaisia aktiivihakemiston ja muita perus ICT-infrastruktuuriin kuvia osa-alueita. Olemassa olevia skriptimallipohjia dokumentaation löytyy markkinoilta, mutta aiheena on rakentaa opinnäytetyötekijän työnantajalle räätälöity ratkaisu.

Tarkoitus on saada samalla kokemusta PowerShell moduulien rakentamisesta, sekä ymmärrystä siitä mitä tietoa oikeasti tarvitsee dokumentoida ja mistä tiedosta on hyötyä. Eli tärkeintä ei ole vain tiedon keräily, mutta myös ymmärrys mitä ko. tiedolla tehdään. Työssä korostuu myös ymmärrys ICT-ympäristön kokonaisuudesta sekä dokumentoitavan tiedon merkitys ja sen hyödyntäminen.

1.4 Käsitteet

Active Directory (AD DS): aktiivihakemisto, Microsoftin kehittämä työkalu käyttäjä- ja konetilien tunnistautumiseen ja pääsynhallintaan.

Domain Controller (DC): Toimialueen ohjauskone. Windows Server palvelin, jolle on asennettu aktiivihakemiston rooli.

Domain Name System (DNS): nimipalvelujärjestelmä.

Windows Server Update Service (WSUS): palvelinrooli, joka hallinnoi Windows työasemien ja palvelinten päivityksiä.

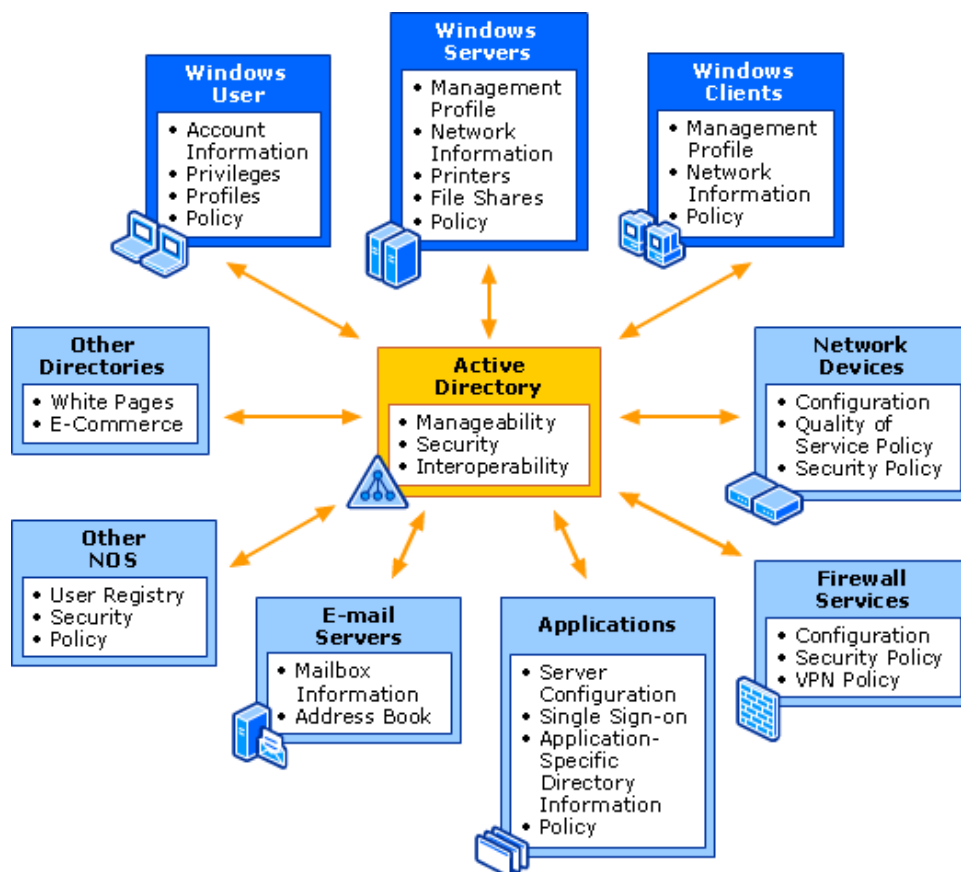
PowerShell: Microsoftin kehittämä skriptausrajapinta, jolla voidaan hallita ja konfiguroida Windows-palvelimia.

Remote Desktop Protocol (RDP): protokolla etäyhteyden muodostamista varten.

2 AKTIIVIHAKEMISTO JA TIETOTURVA

Internetin ja tietokoneiden buumissa 90-luvulla keskisuurten ja suurten yritysten haasteeksi osoitautui kasvavien ICT-ympäristöjen hallinnointi. Vuosituhannen alussa alkuunsa saanut Active Directory oli edelleen oleellinen työkalu Windows-toimialueen työasemien ja palvelinten hallinnoinnissa.

Aktiivihakemiston perustehtävänä oli käyttäjätunnusten ja konetilien hallinnointi. Nykyään kuitenkin muutkin Microsoft Windows palvelinroolit ja ominaisuudet kuten DNS, GPO, DHCP, WSUS ovat täysin riippuvaisia aktiivihakemistosta. Palvelu toimii tietokantana näiden eripalvelujen välillä sallittaakseen eri kone- tai käyttäjätileille pääsyä eri järjestelmiin organisaation ICT-ympäristössä. (Microsoft, Active Directory Domain Services Overview, 2017)



KUVA 1. Aktiivihakemiston rakenne Windows Server Networkissa (Microsoft, Active Directory Collection, 2014)

Kuvassa yksi, keskellä keltaisessa laatikossa sijaitsee aktiivihakemisto, jota ympärillä olevat komponentit käyvät tunnistautumassa. Tyypillinen esimerkki aktiivihakemiston käytöstä löytyi isojen ja keskisuurien organisaatioiden työympäristöstä. Käyttäjien kirjautuessaan käyttäjätunnuksilleen, käyttäjätili validoidaan aktiivihakemistossa, onnistuneessa kirjautumisessa käyttäjä pääsee organisaation toimialueella olevalle työasemalle, eli sisäverkkoon.

Windows-palvelimien ympäristössä, autentikointi tapahtui myös aktiivihakemiston avulla. Kun palvelin validoi käyttäjätunnusta ja konetiliä aktiivihakemistossa. Onnistuneen sisäänkirjautumisen jälkeen, käyttäjä pääsee palvelinympäristöön. Tästä syystä on tärkeää dokumentoida aktiivihakemiston käyttöä, jotta kriittisiltä tietoturvahingoilta välttyttäisiin.

Kuvassa yksi huomataan, jos organisaation muut sisäverkon palvelut ovat integroitu aktiivihakemistoon, niin pahimmillaan ulkopuolinen käyttäjä tai mustahattuhakkeri pääsisivät myös aktiivihakemiston lisäksi muihin sisäverkon järjestelmiin.

Aktiivihakemisto oli tietoturvan kannalta isoin hyökkäysrajapinta yrityksessä. Sen tietoturva on yritykselle äärimmäisen tärkeää myös tietovuotojen ja hyökkäysten takia. Aktiivihakemistoon pääsy mahdollistaa hyökkääjälle pääsyyn kaikkiin organisaation palveluihin, jotka olivat AD-riippuvaisia. (Microsoft, Active Directory Collection, 2014)

2.1 Aktiivihakemiston tietoturva

Kuten aikaisemmassa kappaleessa tuli ilmi, aktiivihakemisto mahdollistaa pääsyyn laajasti erilaisiin aliverkkoihin ja muihin aktiivihakemistoon liitettyihin järjestelmiin. Tämä loi tarpeen luoda kovennettuja tietoturva-asetuksia, jotta aktiivihakemisto pysyisi mahdollisimman turvallisena ja toimintakykyisenä.

Aktiivihakemiston päädyttyä väärin käsiin, voivat vahingot olla hyvinkin mittavat. Hyökkääjää ei välttämättä huomattu heti, jolloin hän pääsi rakentamaan itselleen ”takaovia” järjestelmään, ja pysymään mahdollisimman näkymättömänä jopa kuukausia. Tämän kaltaisia hyökkäyksiä oli tapahtunut sekä maailmalla, että Suomessa, mutta tarkkaa ja luotettavaa tietoa hyökkäyksien määrästä ei ole ollut saatavilla.

Yksityinen yritys, Semperis, oli tehnyt kyselytutkimuksen vuonna 2020, suurilta IT-alan johtajilta liittyen aktiivihakemiston tietoturvaongelmiin. Kyselyyn vastanneista ilmoittivat, heidän toimintansa oli edelleen riippuvainen aktiivihakemistosta, ja siihen integroiduista palveluista. (Semperis, 2020)



KUVA 2. Semperis-yrityksen kyselytutkimuksen osallistuneiden henkilöiden vastaukset, liittyen aktiivihakemiston käytöstä heidän organisaatioissaan. (Semperis, 2020)

Kuvassa kaksi on kyselytutkimuksesta saatu tulos, missä tutkimukseen osallistuneet IT-alan asiantuntija vastasivat, kuinka paljon heidän yrityksessään käytetään edelleen aktiivihakemistoa. Tutkimustuloksista ilmeni, että lähes kaikki vastanneista asiantuntijoista käyttävät aktiivihakemistoa jossakin määrin heidän yrityksessään.



KUVA 3. Semperis-yrityksen kyselytutkimuksen osallistuneiden henkilöiden vastaukset, liittyen aktiivihakemiston katon vaikutuksesta organisaatioon. (Semperis, 2020)

Kuvassa kolme nähdään, että aktiivihakemiston katkoksen aikana, vaikutukset voivat olla hyvinkin merkittäviä. Lähes kaikki vastanneista asiantuntijoista ilmoittivat, että aktiivihakemiston kaatuessa, sen vaikutukset näkyvä organisaatiossa jollakin tavalla. Myös kolmasosa vastanneista ilmoittivat, että jälkiseuraukset olivat hyvinkin kriittisiä organisaatiolle, jolloin vahingot olisivat voineet olla merkittäviä. (Swinhoe, 2019)

Verkosta löytyi monia esimerkkejä, kuinka tämänkaltaisen vahinko vaikuttaisi organisaation toimintaan sekä taloudellisesti että operationaalisesti. Lunnasohjelmien trendin kasvaessa, hyökkäyksien kohteeksi olivat usein joutuneet yritysten Domain Controller palvelimet. Esimerkiksi yksiä suurimpia kontti- ja toimituspalvelusten toimijoista maailmalla Maersk ilmoitti viime vuonna heihin kohdistuneesta aktiivihakemisto-hyökkäyksestä, josta koitui suuria vahinkoja kyseiselle yhtiölle. Vuonna 2017 Not-Petya niminen haittaohjelma lamaannutti ja aiheutti katkoksen Maerskin aktiivihakemistoon, jonka seurauksena heidän piti rakentaa heidän aktiivihakemistonsa uudelleen. Laivayhtiön IT-johtaja Andy Powell, kertoi oppivansa paljon aktiivihakemiston 9-päiväsen katkon aikana. Hän korostaa tämän kaltaisissa hyökkäyksissä kykyä palautua normaalitilaan mahdollisimman nopeasti. Tämänkaltaisen palautuminen oli mahdollista hyödyntämällä disaster recovery-suunnitelmaa, ja siihen liittyviä dokumentaatiota. (Swinhoe, 2019) (Semperis, 2020)

2.2 Aktiivihakemiston palautus ja testaamisen ongelmat

Disaster recovery, on organisaation itsensä laatima sisäinen hätäpalautussuunnitelma, joka noudattaa organisaatiota omaa palautusjärjestystä. Hätäpalautussuunnitelmassa käsitellään organisaation Domain Controller-palvelimia, niiden varmuuskopiointia ja erityisesti varmuuskopioinnin palautusjärjestystä ja säilömismenetelmiä. On tärkeää myös huomioida suunnitelman ajantasaisuutta ja testata sen toimintoja tietyin väliajoin (vuosikellon mukaisesti). Siispä palautus voidaan toteuttaa monella eri tavalla, mutta Domain Controllerin palauttaminen ei ole yksinkertainen toimenpide, toiminto vaatii erityisiä organisaation sisäisiä ohjeita. Windows Server-palvelin, joka suorittaa AD DS -toimintoa (Active Directory Domain Service), kutsutaan "Domain Controller" (Microsoft, 2019)

Semperis mainitsi vuoden 2020 elokuun tiedotteessaan, että aktiivihakemiston palautukseen liittyvien epäonnistumisien määrä on suuri. Hajautettua arkkitehtuuria ja "multi-master"-kopiointia hyödynnetään monissa perinteisissä hätäpalautussuunnitelmissa, jolloin palauttaminen onnistui suhteellisen helposti. Kuitenkin on mahdollista, että lunnasohjelma tai jokin muu haittaohjelma korruptoi kaikkien Domain Controllerien kiintolevyt, jolloin kaikki tieto poistetaan yhdestä kerrasta. Tästä syystä aktiivihakemiston rakenteen palauttaminen ei välttämättä ole mikään yksinkertainen toimenpide. Microsoft tarjoaa pitkän ja monimutkaisen teknisen ohjeen, jossa opastetaan aktiivihakemiston rakenteen palauttamisen, mutta tässäkin tapauksessa palautuksen onnistumisesta ei tiedetä, ennen kuin toiminto on suoritettu loppuun. Semperis oli järjestänyt myös erillisen harjoitusskenaarion, missä palautuksen epäonnistuminen oli yli 80 %. (Semperis, 2020)

Toinen yleinen ongelma hätäpalautussuunnitelmassa on sen testaaminen. Semperisin kyselytutkimuksessa tuli ilmi myös se, että monet organisaatiot eivät ole todellisuudessa testanneet heidän suunnitelmaansa. Kuvassa neljä on kyselytutkimuksen tuloksia, josta nähdään, että kolmas osa organisaatioista on luonut suunnitelman, mutta eivät ole ikinä testanneet sitä. Ainoastaan viisi prosenttia kyselyyn vastanneista kertovat testanneensa palautuksen toimivuutta onnistuneesti viimeisen kahdentoista kuukauden aikana. Tutkimuksessa myös ilmeni, että juuri suunnitelman testaamatta jättäminen herättää organisaatioissa eniten pelkoa, jos he joutuvat kyberhyökkäyksen kohteeksi. (Semperis, 2020)



KUVA 4. Semperis-yrityksen kyselytutkimuksen osallistuneiden henkilöiden vastaukset, liittyen heidän organisaatioiden hätäpalautussuunnitelman testauksesta. (Semperis, 2020)

2.3 Yleisimmät hyökkäykset aktiivihakemistoa vastaan

Seuraavissa luvuissa käsitellään hyökkäyksen ensikontaktia, jossa käsitellään erilaisia hyökkäystapoja, niiden aiheuttamia tapahtumaketjuja ja niistä aiheutua seurauksia sisäverkossa. Lopuksi käsitellään mahdollisia hyökkääjän aiheuttamia vahinkoja ja mahdollisia takaovien luonti järjestelmään.

2.3.1 Hyökkäyksen ensikontakti

| Menetelmä | Kuvaus |
|--|--|
| Tietojenkalastelu (eng. Phishing) | Jaettavissa kahteen eri alalajiin, kohdennettuun ja kohdentamattomaan. Kohdennetussa menetelmässä, lopullinen uhri on tiedossa. Tässä menetelmässä myös hyödynnetään paljon sosiaalisia tekniikoita, missä pyritään manipuloimaan ja saavuttamaan haluttuja tuloksia puhumalla/kirjoittamalla. Kohdentamattomassa kalastelussa lähetetään roskapostia laajalle joukolle ihmisiä, jossa pyritään saaman henkilötietoja / tunnuksia. |
| Ulospäin näkyvät palvelut (esim. VPN) | Etäyhteyspalvelut, Citrix-virtualisointipalvelut ja Windows Remote Management. Ulospäin näkyvien palveluiden haavoittuvuuksia hyödyntäminen, jossa hyökkääjä pyrkii hyödyntämään tiedossa olevaa haavoittuvuutta. |
| Fyysinen taso (eng. Hardware) | Lisälaitteet, ajureiden haavoittuvuudet ja WLAN-verkko. Hyökkääjät pyrkivät hyödyntämään tiedossa olevia haavoittuvuuksia ja kaappaamaan uhrin työaseman hyödyntäen näitä menetelmiä. |
| Ulkoiset mediat (esim. USB) | Haittaohjelmien levittäminen fyysisessä muodossa. Esimerkiksi käyttäjä asentaa tietämättään RATs (Remote Access Trojan) haittaohjelman, jolloin hyökkääjä pääsee ottamaan yhteyttä uhrin työasemaan. |

TAULUKKO 1. Erilaisia tapoja luoda ensikontakteja hyökkääjän ja uhrin välillä. (ATT&CK, 2018)

Taulukossa yksi käsiteltiin yleisimpiä haittaohjelman luomia ensikontaktiin liittyviä menetelmiä. Mutta kuinka käyttäjät pystyvät suojautumaan erilaisilta uhkilta? Tietojenkalastelu on globaalisesti tunnetuin tapa hankkia tietoa kohteilta. Tehokkain keino suojautua tietojenkalastamiselta on kouluttamalla henkilöstä erottamaan kalasteluviestejä tavallisista viesteistä. On tärkeätä, että käyttäjät eivät mene harhaan ja ovat tietoisia liikkeellä olevista uhkista ja niiden näyttäytymistavoista. Paras tapa taas suojautua ulospäin näkyviltä palveluilta, on asentaa tuoreimpia päivityksiä ja noudattamaan tuoreimpia tietoturva-asetuksia. Fyysisen tason suojautuminen onnistuu parhaiten välttämällä tuntemattomien laitteiden liittämistä työasemaan ja välttämällä tuntemattomia ja julkisija verkkoja. Sama sääntö voidaan noudattaa ulkoisten medialaitteiden kanssa. (Commission, 2019)

2.3.2 Sisäverkossa eteneminen



KUVA 5. Aktiivihakemiston hyökkäyksen anatomia. (Mera, 2020)

Aikaisemmassa luvussa käsiteltiin erilaisista hyökkäyksen alkupisteistä, joita kutsutaan ensimmäisiksi yhteyksiksi. Yleisimmät tavat luoda ensikontakti oli tietojenkalastelulla tai raakahyökkäyksellä (eng. brute-force). Uuden nykystandardin mukaan, loppukäyttäjän aktiivihakemiston salasana täytyy olla vähintään 14-merkkiä. (Mera, 2020)

Kuvassa viisi, käsitellään esimerkitapausta korkeantason hyökkäyksestä. Hyökkäys eskaloituu viidessä eri jaksossa (Mera, 2020):

- 1. Tilien kaappaaminen raakahyökkäyksen avulla**
 - Tämä taso läpäistään, mikäli organisaatiossa on sallittuna heikot ja yleiset salasanat.
 - Kirjautuminen tapahtuu epätavallisesta IP-osoitteesta, outoina ajanhetkinä ja vieraasta järjestelmästä.
- 2. Horisontaalinen liikkuminen aktiivihakemiston hierarkiassa**
 - Useita kirjautumisia yhdeltä IP-osoitteelta.
 - Mikäli hyökkääjä pääsee luomaan yhteyden yrityksen verkkoon ja työasemiin, joissa järjestelmänvalvojan tunnus on kaikissa työasemissa sama, hyökkääjä pääsee horisontaalisesti koko ympäristössä. Vaikeuttaakseen hyökkääjän liikkumista ympäristössä, on käytteenotettava LAPS-ominaisuus (Local Admin Password Solution).
- 3. Hyökkääjä onnistuu korottamaan oikeuksiaan**
 - Aktiivihakemiston käyttäjätunnus on lisätty oikeusryhmään.
 - Mikäli työasemalle on kirjaututtu korkeamman tason oikeuksilla, hyökkääjä pääsee kaappaamaan kyseiset tunnuksset, ja täten korottamaan omia oikeuksiaan ympäristössä.
 - Microsoft on tarjonnut uudet tasomallin implementoitavaksi aktiivihakemistoon. Ajattelumallilla pyritään ehkäisemään vertikaalista liikkumista, jolloin käyttäjät eivät

pysty korottamaan omia oikeuksiaan. Ajatusmallin tarkoituksena on antaa käyttäjille ainoastaan heille tarvittavan määrän oikeuksia tasoittain. (Microsoft, 2019)

- i. Taso 0 on tarkoitettu palvelin- ja rautatasoksi.
 - ii. Taso 1 on taustapalvelut.
 - iii. Taso 2 on työasemien järjestelmänvalvojille.
4. Hyökkääjä luo takaoven järjestelmään ja lisää itselleen oikeuksia
- Uuden käyttäjätilin luonti ja sen lisääminen oikeusryhmään.
 - Hyökkääjä pääsee hyödyntämään "Pass-The-Hash"- tai "Pass-The-Ticket"-tyyppisiä tekniikoita yrittääkseen korottaa omia oikeuksiaan järjestelmässä.
5. Halutun tiedon varastaminen
- Pääsy suureen määrän tietoon ja epätavallisten laitteisiin pääsy.
 - Hyökkääjä pääsee luomaan itselleen "takaovia" järjestelmään myöhemmäksi käytettäväksi.

Neljännessä sarakkeessa mainittiin "Pass-The-Hash"- tai "Pass-The-Ticket". Näiden menetelmien tarkoituksena on päästä hyödyntämään tunnustilejä pahantahtoisesti laajemmissa mittamäärissä. "Pass-The-Hash"-menetelmässä, hyökkääjä pyrkii kaappaamaan haittaohjelman avulla loppukäyttäjän salasanan hash-version. Hashillä tarkoitetaan sitä, että jokin teksti tai salasana on ajettu yksisuuntaisen funktioalgoritmin läpi, jolloin lopputulotteksi syntyy pätkä satunnaisia merkkejä, joista ei voida selvittää alkuperäistä tekstiä tai salasanaa, mutta sitä voidaan silti käyttää joissakin muissa tapauksissa. Lopputuloksena, hyökkääjällä on käsissään hajautettu versio salasanasta, jolla hän pääsee esittämään kyseistä tunnusta. "Pass-The-Ticket"-menetelmässä hyökkääjä pystyy väärentämään viimeisimmän kirjautuneen henkilön käyttäjätunnusta, jotta hän pääsisi autentikoitumaan Windows palvelimelle Kerberos-tiketin avulla. Tällä menetelmällä on samanlaiset vaikutukset kuin edelliselläkin. (Swedin, 2014) (Hasayen, 2019)

Nämä menetelmät pohjustava seuraavia tunnetuimpia menetelmiä, joita yhdistää konetilin ja käyttäjätunnuksen kaappaamine (Sarode, 2020):

| Menetelmä | Kuvaus |
|---------------|--|
| Golden Ticket | Aktiivihakemistossa, käyttäjätunnukset voivat palauttaa joissakin tapauksissa kerberostiketin, joka sisältää todennustunnuksen. Tätä todennustunnusta käyttämällä, hyökkääjä pääsee autentikoitumaan KRBTGT tunnusta, joka on erillinen salattu tili, jolla voidaan väärentää / esittää muita käyttäjätilejä. (Petters, 2020) |
| Silver Ticket | Silver Ticket, on väärennetty todennustunnus, jolla päästään suoraan ohittamaan domain controlleri. Tämä mahdollistaa suoran kommunikoinnin työaseman ja palvelimen välillä. Tämän kaltainen menetelmä on mahdollista, koska väärällä autentikoidulla tiketillä on mahdollista kirjautua, ilman että Kerberos tupla tarkistaa autentikoitumista. (Petters, Kerberos Attack: Silver Ticket Edition, 2020) |
| DCSync | Tässä menetelmässä, hyökkääjä simuloi domain controllerin toimintoja, jonka avulla hän pääsee käsiksi palautettuihin salasanatietoihin hyödyntämällä domainin replikaatiota. Kun hyökkääjä on saanut oikeudet yksi- |

| | |
|--------------|--|
| | tyisiin tunnuksiin domainin replikaation oikeuksilla, hän pääsee hyödyntämään erillisiä protokolia, joilla pystytään jäljentämään domain controlleria. (Berg, 2019; Commission, 2019) |
| DSRM Account | DSRM Account, eli Directory Restore Mode Account, on menetelmä, jossa hyökkääjä onnistuu kaappaamaan DSRM-tilin. Tämä tilin tarkoituksena on toimia domain controllerin paikallisena järjestelmänvalvojana, jonka salasanaa harvemmin päivitetään asennuksen jälkeen. DSRM-tili mahdollistaa kirjautumisen domain controlleriin ja pahimmillaan pääsyn koko verkkoon hyödyntämällä "Pass-the-Hash"-menetelmää. (Metcalf, 2015) |

TAULUKKO 2. Erilaisia menetelmiä, joilla pyritään etenemään sisäverkossa.

Tunnetuimpien menetelmien päätavoitteena on kaapata "Domain Admin" tunnuksien, koska niiden mahdollistamat oikeudet tarjoavat erinomaiset mahdollisuudet hyökkääjälle pääsemään aktiivihakemiston kriittisimpiin osiin. Tämä synnyttää tarpeen dokumentoida ja seurata tunnuksien olemassaoloa ja käyttöä, jotta aktiivihakemistossa ei olisi yhtäkään ylimääräistä järjestelmänvalvojan tunnusta käytössä. (Metcalf, The Most Common Active Directory Security Issues and What You Can Do to Fix Them, 2015)

2.3.3 Hyökkäyksen vahingot ja sen motiivit

Hyökkääjän motiivina voi olla monia eri syitä. Esimerkiksi hyökkääjän tarkoituksena voi olla tietojen anastaminen ja niiden myyminen pimeillä markkinoilla tai takaovien luonti järjestelmään myöhempiä iskuja varten. Monet sadat yritykset ympäri maailmaa ovat jatkuvasti uhattuina, koska monet kilpailijat ja rikolliset ovat kiinnostuneita heidän yrityssalaisuuksistaan. Yrityksiä vastaan kohdistuu myös yleistä härnäämistä, jonka tarkoituksena on aiheuttaa yritykselle tappiota ja sabotoida heidän yritystoimintaansa. Härnäämisessä korostuu myös hyökkääjän omien taitojen näyttäminen ja rajojen kokeilemista vieraissa ympäristöissä. (Grimes, 2010)

2.4 Yleisimmät suojautumismekanismit

Edellisessä luvussa mainittujen tekniikoiden päätavoitteena oli Domain Admin -tunnusten kaappaminen. Tämä oli synnyttänyt tarpeen luoda perusteellisia suojautumismekanismeja, jotta haittaohjelmien ja hyökkääjien pääsyä estettäisiin aktiivihakemistoon. Esimerkiksi oli tärkeätä dokumentoida ja seurata ettei Domain Admin -tunnuksia olisi aktiivihakemistossa olleenkaan.

| | Haitat | Suojautuminen |
|-------------------------------|--|--|
| Domain Admin tunnuksien määrä | Mitä enemmän järjestelmänvalvojan tunnuksia järjestelmässä on liikenteessä, sitä isompi riski on, että niitä hyväksikäytetään. | Järjestelmänvalvojan tunnuksien määrää rajoitetaan, ja niiden käyttö sallitaan ainoastaan niille henkilöille, jotka tarvitsevat sitä jokapäiväisessä työssään. |
| Heikot salasanat | Liian heikot salasanat mahdollistavat helpon pääsyn tileille. Kohdistetussa hyökkäyksessä | Nykystandardissa määritellään, että salasanan minimipituus on 14 merk- |

| | | |
|---|---|--|
| | salasanan murtaminen voi onnistua hyvinkin lyhyessä ajassa, jos salasana ei ole vahva. | kiä. Tämä mahdollistaa tarpeeksi monimutkaisen salasanan, jolloin salasanan murtamiseen voi olla käytännössä mahdotonta. |
| Liikaa oikeuksia Service-tunnuksilla | Kaappauksen tapahtuessa, mahdollisuus edetä hyvinkin pitkälle verkkojärjestelmässä. | Service-tunnuksien todellista merkitystä pitää huomioida, ja rajoittaa sen oikeuksia sen mukaisesti. Service-tunnuksien kohdentaminen tiettyihin järjestelmiin tuo entistä enemmän turvallisuutta järjestelmään. |
| Tunnusten delegointi | Turhien tunnusten delegoiminen aiheuttaa suurempaa riskiä järjestelmälle, joutua hyökkäyksen kohteeksi. Liiallinen tunnuksien delegoiminen, mahdollistaa hyökkäyksien rakentamista. | Järjestelmätunnuksien salasanojen päivitykset ja niiden kohdentaminen tarvittaviin järjestelmiin mahdollistavat paremman turvallisuuden järjestelmälle. |
| Ylimääräiset roolit domain controllerilla | Mitä vähemmän ylimääräisiä rooleja domain controllerilla on, sitä pienempi hyökkäysriski on järjestelmään vastaan. | Ylimääräisten roolien poistaminen domain controllerilta, jotta hyökkäysriskin määrä olisi mahdollisimman vähäinen. |
| Vanha käyttöjärjestelmä | Vanhojen käyttöjärjestelmien haavoittuvuuksia löydetään ajan saatossa ja niiden päivitykset on pahimmassa tapauksessa lopetettu. | Käyttöjärjestelmien ajantasaisuus vähentää hyökkäysriskiä. |
| LAPS-ominaisuus | Mikäli kaikissa työasemissa on sama järjestelmänvalvojatunnus ja LAPS-ominaisuus ei ole käytössä, hyökkääjä pääsee liikkumaan järjestelmässä horisontaalisesti. | LAPS-ominaisuuden käyttöönotto vaikeuttaa horisontaalisen liikkumisen järjestelmässä. |
| Aktiivihakemiston tunnuksilla kirjautuminen | Mikäli työasemalle on tallentunut aikaisempi kirjautuminen korkeampi tasoiselta tililtä | Microsoftin tasomallin implementointi aktiivihakemistoon. |

| | | |
|--|---|--|
| työasemiin ja muhin palvelimiin | (enemmän oikeuksia), hyökkääjällä on mahdollisuus kaapata tämän tilin hashi. | |
| Kriittisen palvelinten pääsy miltä tahansa pisteestä | Mikäli verkkotason pääsyä ei ole estetty, hyökkääjä pystyy muodostamaan yhteyden kriittiseen palvelimeen. | Pääsy palvelimen verkkotasolla on estetty. |
| Käyttämättömien tunusten säilyttäminen | Mahdollistaa potentiaalisen ja huomaamattoman väärinkäytön. | Käyttämättömien tilien poistaminen käytöstä. |

TAULUKKO 3. Taulukoitu erilaisia tapoja parantaa Domain Controllerin tietoturva, ja suojaamattomuuden aiheuttamia haittaesimerkkejä. (Metcalf, The Most Common Active Directory Security Issues and What You Can Do to Fix Them, 2015)

3 DOKUMENTAATIO

Tässä luvussa käsitellään dokumentoinnin tarvetta ja sen rakentamista aktiivihakemiston ylläpitoa varten. Dokumentaation tarve yritykselle korostuu siinä vaiheessa, kun yrityksen täytyy analysoida ja auditoida omaa järjestelmäänsä. Esimerkiksi kahden yrityksen fuusioinnissa syntyy kaksi erillistä järjestelmää, jotka pitää yhdistää yhdeksi yhtenäiseksi kokonaisuudeksi. Puutteellinen dokumentaatio tuottaa ylimääräistä työtä, vaikeuttaa fuusioitumista ja vaikeuttaa tulevaisuudessa järjestelmien ylläpitoa. Toinen tyypillinen esimerkki löytyy myös yritysmaailmasta, missä järjestelmän hätäpalautussuunnitelman toteuttaminen vaikeutuu, jos yrityksellä ei ole ennalta suunniteltua palautusohjetta. Sekä IT-ylläpitäjien vaihtuessa olisi dokumentointi suotavaa, helpottaakseen nykytilan esittelyä.

Dokumentoimalla aktiivihakemisto, voidaan saada suuriakin etuja:

- Vianselvitykset pystytään suorittamaan yksinkertaisemmin ja tehokkaammin.
- Vikatilanteen sattuessa, palautuminen on mahdollista.
- Mahdollisuus löytää implisiittisiä asetuksia.
- Yhtenevä yleiskuva järjestelmästä ja sen tietoturvasta.
- Helpottaa tiedon- ja järjestelmän siirtämistä ylläpitäjien välillä.

3.1 Puutteellisen dokumentaation vaikutus

Edellisessä kappaleessa käsiteltiin dokumentaation vaikutusta yrityksentoimintaan, jos sellaista ei yrityksestä löydy tai se on vanhentunut/puutteellinen. Tässä luvussa käsitellään dokumentaation vaikutuksesta ja siihen liittyviä työkaluja ja esimerkkitapauksia.

Aikaisemmassa pääluvussa käsiteltiin disaster recoverya, eli hätäpalautussuunnitelmaa. Tämän suunnitelman tarkoituksena on palauttaa vioittunut, kaapattu tai kokonaan poistettu järjestelmä. Samaisessa luvussa myös käsiteltiin sitä, että monet yritykset ovat laatineet tämänkaltaisen hätäpalautussuunnitelman, mutta eivät ole ikinä testanneet sen toimintoa, tai ovat edes varmoja onko suunnitelma ajantasainen. Tässä on loistava esimerkki siitä, kuinka tärkeitä on dokumentoida aktiivihakemistoa ja siihen integroituneita järjestelmiä, jotta palautuksesta saataisiin mahdollisimman eheä. Tutkimuksessa myös ilmeni se, että palautuksen onnistumisprosentti oli hyvin pieni, eli ajantasaisella dokumentoinnilla pyritään ehkäisemään suurempi haittavaikutuksia, jos järjestelmä kaatuu.

Tärkeä huomioon otettava ilmiö dokumentoinnissa oli implisiittiset asetukset, joidenka merkitys oli korostunut turvallisuudessa. Varisinkin järjestelmäylläpitäjän vaihtuessa, juuri näiden kaltaisten asetusten ylös kirjaaminen mahdollistivat sulavan ja eheän vaihdoksen kahden ylläpitäjän välillä. Tyypillinen esimerkki tämän kaltaisesta implisiittisestä asetuksesta oli rooliryhmien delegoiminen, jolloin uudelle ylläpitäjälle oli hyvinkin epäselvää, minkälaisia oikeuksia liikkuu missäkin rooliryhmissä.

3.2 Dokumentoinnin rakentaminen

Kuten aikaisemmissa luvuissa oli todettu, aktiivihakemistolla oli merkittävä rooli yritysten rakenteessa. Moni näistä yrityksistä päivittivät heidän aktiivihakemistoaan vasta domain controllerin käyttöjärjestelmän päivittämisellä. Aktiivihakemisto oli suunniteltu alusta lähtien siihen, että se on mahdollisimman yhteensopiva vanhempienkin järjestelmien kanssa. Tämä jätti suuren määrän vanhoja protokolia ja asetuksia roikkumaan aktiivihakemiston elinkaareen. Tästä syystä monissa aktiivihakemistoissa oli tapahtunut tyypillinen ilmiö, missä käyttöjärjestelmää päivitettiin tietyin väliajoin, mutta vanhat asetukset ja protokolat olivat edelleen käytössä. (Loos, 2019)

Dokumentaation rakentamisessa on otettava huomioon dokumentaation ikääntyminen ja monia muita tekijöitä. Pitää olettaa, että sisäverkon tavallinen käyttäjä pystyy tekemään virheitä ja luomaan tätä kautta vaaratilanteita järjestelmälle. Tästä syystä on tärkeitä muistaa ylläpitää dokumentaatiota, jotta tulevaisuudessa välttyttäisiin ongelmilta ja mahdollisilta hyökkäyksiltä. Dokumentaation ajantasaisuutta voidaan parantaa automatisoimalla dokumentaation laadinta sovelluksilla. (Loos, 2019)

Jokaisen uuden käyttöliittymäpäivityksen myötä, Microsoft oli julkaissut sarjan uusia päivityksiä, parannuksia, ja parantanut aktiivihakemiston vakautta ja palautumiskykyä. Mutta moni näistä ominaisuuksista vaatii erillisiä toimenpiteitä, jotta niiden implementointi yrityksen aktiivihakemistoon onnistuu turvallisesti. (Loos, 2019)

4 TYÖN SUUNNITTELU

Tässä pääluvussa käsitellään opinnäytetyön suunnittelu osiota, missä käsitellään toimeksiantajan ja opinnäytetyöntekijän asettamia minivaatimuksia, työhön sisältyviä dokumentaatioehtoja ja niiden muotoja sekä ohjelmakoodin modulaarisuutta ja elinkaarta jatkokehityksen kannalta. Viimeisessä luvussa pohditaan ja käsitellään testiympäristön pystyttämistä ja sen tarvittavia toimintoja.

4.1 Työn minimivaatimukset ja rajaus

Työn lopputuloksena, oli tarkoitus tuottaa yksinkertainen ohjelmamoduuli, jolla pystyttäisiin hakemaan erilaisia tietoja palvelimista ja ICT-infrastruktuurista. Moduulin oli oltava vähintään yhteensopiva PowerShell 5.1 -skriptausrajapinnan kanssa. Moduuli toimi palvelinympäristössä, jonka toiminnosta kerrotaan myöhemmässä luvussa. Moduulin oli pystyttävä myös tulostamaan haettua tietoa joko JSON- tai HTML-formaatissa.

Opinnäytetyön tarkoituksena oli tuottaa yksinkertainen ja toimiva moduuli asiantuntijoiden käyttöön, jota pystyttäisiin myöhemmässä ajankohdassa jalostamaan tarvittaessa. Moduulia ei kehitetty kaupalliseen käyttöön, eikä sen käyttömukavuuksiin panostettu tässä työssä. Sovellusta ohjattiin kommentteja kehotteen avulla, ilman mitään erillistä graafista käyttöliittymää.

4.2 Aikataulu ja projektin kulku

Sovelluskehityksessä toteutettiin ketterästi. Toteutus suoritettiin loppuun vuoden 2020 lopulla. Projektin kulkua oli kronologinen, eli alussa pohjustettiin kaikki tarvittavat kehitysympäristöt ja toiminnot, jonka jälkeen valmistettiin ohjelmamoduuli ja kokeiltiin sen toimintoja lopuksi.

4.3 PowerShell-moduuli

Aikaisemmassa luvussa mainittiin moduulin jatkokehityksestä ja sen modulaarisuudesta. Ohjelmakoodin rakenteessa pyrittiin noudattamaan kaikkia mahdollisia hyviä käytäntöjä, joita kouluopintojen aikana oli opeteltu. Valitettavasti PowerShellin arkkitehtuurista ei löydy virallista standardia, joten sovelluksen kehittämisessä käytettiin verkosta löytyneiden asiantuntijoiden hyväksi todettuja käytäntöjä ja oppeja.

Miksi moduulin käyttö PowerShellissä? Moduulin ohjelmarakenne oli yksinkertainen, ja se soveltui erinomaisesti tämänkaltaiseen työhön, missä haluttiin modulaarisuutta ja yksinkertaisuutta.

Skriptimoduuli oli mikä tahansa validi PowerShell-skripti tallennettuna .psm1 -tallennusmuotoon. Tämä tallennusmuoto sallii PowerShell moottorin sääntöjen ja moduulien funktioiden käytön moduulissa. Moduulissa voitiin hyödyntää Microsoftin komponentteja helpottaakseen skriptin ajoa ja debugausta. (Microsoft, 2019)

Mitä moduulin luomiseen tarvittiin? Moduuli voitaisiin luoda monella eri tavalla, kuten liittämällä .psd1-laajennus tiedostoon tai kokoamalla toimiva binäärimoduuli C#:lla. Tässä työssä moduuli rakennettiin seuraavista komponenteista:

- Moduulin manifesti, jossa kuvataan moduulin käyttötarkoitus ja auktori.
- Juuri moduuli, tarvitaan moduulin asennuksessa.
- Julkiset funktiot, erilaisia funktioita, joita loppukäyttäjä pystyy suorittamaan.
- Privaatti funktiot, vapaavalintaisia apufunktioita, joita loppukäyttäjä ei pysty käyttämään.
- Formaattit, vapaavalintainen formaatti, jonka avulla voidaan muokata tuloksen esitysmuotoa.
- ReadMe, osa GitHubin tai muiden arkistointityökalujen käyttöä.

(Frame, 2016; Frame, 2016)

4.4 Kehitysympäristö

Ohjelmamoduulin kehitystä ja testausta varten rakennettiin erillinen virtuaalipalvelinympäristö Microsoft Azure pilvipalveluun. Testauspalvelimena toimi yksi toimialueen ohjauskone (Domain Controller) - Windows Server 2016 palvelin. Koodin kehitysympäristönä käytettiin Microsoft Visual Code.

5 TYÖN TOTEUTUS

Työn toiminnallisessa toteutuksessa, päästiin syvemmälle opinnäytetyössään. Lopullinen työ oli monipuolisempi kuin alustavassa suunnittelussa oletettiin. Tästä syystä opinnäytetyöraportissa työn toteutus oli laajempi kuin suunnittelussa. Seuraavissa luvissa käsitellään työn etenemistä kronologisessa järjestyksessä.

5.1 Kehitysympäristön alustaminen ja ohjelmakoodin hallinnointi

Kehitysympäristönä käytettiin Azure-pilvipalveluita. Pilvialustalle asennettiin yksi Windows Server 2016 palvelin Domain Controller tarkoitukseen. Yhteys palvelimeen muodostettiin RDP-ohjelman välityksellä.

| | |
|---------------------------|------------------------|
| Virtual machine | |
| Computer name | WinAD16 |
| Operating system | Windows |
| Publisher | MicrosoftWindowsServer |
| Offer | WindowsServer |
| Plan | 2016-Datacenter |
| VM generation | V1 |
| Agent status | Not Ready |
| Agent version | Unknown |
| Host | - |
| Proximity placement group | N/A |
| Colocation status | N/A |

KUVA 6. Kehitysympäristön palvelimen perustiedot.

Koodia hallinnointiin GitHub-ohjelmistoversiohallintapalvelussa. Tässä vaiheessa alustettiin myös kaikki tarvittavat tiedostot GitHubissa, kuten ReadMe.

5.2 Tiedon keruu

Tiedon keruu järjestelmästä tapahtui kutsumalla PowerShell skriptiä. Koodipohjana oli käytetty myös muita valmiina olevia koodipohjia sekä valmiita Microsoftin moduuleita kuten Get-DnsServerZone. Kuvassa seitsemän on esimerkki tästä koodinpätkästä.

```
$DnsServerZone = Get-DnsServerZone |
    ConvertTo-Html
    -Property ZoneName,
    ZoneType,
    IsAutoCreated,
    IsDSIntegrated,
    IsReverseLookupZone,
    IsSigned -Fragment -PreContent "<h2>DNS Server Zone</h2>"
```

KUVA 7. PowerShell-skriptillä DNS tietojen hakeminen ja niiden tallennus HTML-muotoon.

Kuvassa 7 on esimerkki DNS tietojen keruusta, jossa muuttuja \$DnsServerZone hakee funktiolla Get-DnsServerZone kaiken halutun tiedon dokumentaatiota varten. Esimerkissä on myös DNS-funktio yhdistetty ConverTo-Html-funktioon, joka generoi tarvittavan HTML-fragmentin. Silloin alkuperäinen muuttuja saa arvoksi automaattisesti HTML-objektin, jota on raporttia generoidessaan helpompi käsitellä.

```

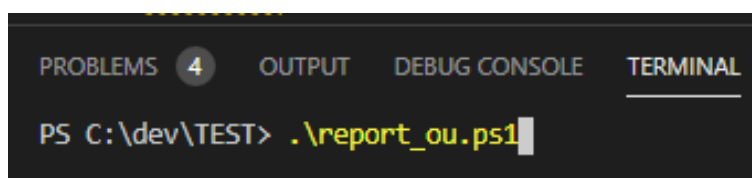
$Report = ConvertTo-HTML
-Body "$DomainName $DnsServerZone $DnsServerZoneAging $DnsServerScavenging"
-Head $header
-Title "DNS Information Report"
-PostContent "<p id='CreationDate'>Creation Date: $(Get-Date)</p>"

#The command below will generate the report to an HTML file
$Report | Out-File .\Basic-DNS-Information-Report.html

```

KUVA 8. PowerShell-skriptillä Eri osa alueiden tulostaminen yhtenäiseksi raportiksi.

Kuvassa kahdeksan generoidaan yhtenäinen raportti kaikissa dokumentoitavista osa-alueista. Raportti tallennetaan HTML-muodossa samaan paikkaan missä sijaitse itse skriptikoodi.



KUVA 9. PowerShell-skriptin suorittaminen koodinkäsittely ohjelmassa.

Kuvassa yhdeksän on esimerkki skriptin ajosta testiympäristössä.

5.3 Dokumentoitava data

Seuraavissa kappaleissa esitetään esimerkkitietoja ja mitä datalla voitaisiin tehdä. Opinnäytetyössä lähdettiin liikkeelle seuraavilla dokumentoitavilla osa-alueilla:

- Domain Controller-tiedot
- DNS-tiedot
- Aktiivihakemisto

5.3.1 Domain Controller tiedot

Palvelimen perustietojen dokumentaatioon koostuu seuraavista objekteista:

- Palvelimennimi
- Käyttöjärjestelmänversio
- Verkkoasetukset
- Palvelimen käynnissäoloaika
- Levynkoot
- Ajastetut tehtävät

Dokumentoimalla perustietoja toimialueen ohjauskoneesta, voi asiantuntija saada paremman yleiskuvan palvelutilasta. Esimerkiksi dokumentaatiosta käy helposti esille toimialueen ohjauskoneen käyttöjärjestelmänversio. Ohjauskoneen käyttöjärjestelmänversio päivitys voidaan ottaa huomioon ICT-ympäristön elinkaarenhallinnassa, mikäli siihen on tarvetta.

Domain Controller name: WinAD16

Operating System Information

| | |
|---------------|--|
| Version: | 10.0.14393 |
| Caption: | Microsoft Windows Server 2016 Datacenter |
| BuildNumber: | 14393 |
| Manufacturer: | Microsoft Corporation |

Processor Information

| | |
|--------------------|---|
| DeviceID: | CPU0 |
| Name: | Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz |
| Caption: | Intel64 Family 6 Model 85 Stepping 4 |
| MaxClockSpeed: | 2095 |
| SocketDesignation: | None |
| Manufacturer: | GenuineIntel |

BIOS Information

| | |
|--------------------|--|
| SMBIOSBIOSVersion: | |
| Manufacturer: | |
| Name: | |
| SerialNumber: | |

Disk Information

| | |
|---------------|---------|
| DeviceID: | C: |
| DriveType: | 3 |
| ProviderName: | |
| VolumeName: | Windows |

KUVA 10. Esimerkki toimialueen ohjauskoneen perustiedon raportista.

5.3.2 DNS-tiedot

DNS on vahvasti kytköksissä DNS:ään Dokumentoidaan testiympäristössä seuraavat nimenselvennys palvelun tiedot:

- DNS alueet
- DNS alueiden vanhentumisasetukset
- DNS tietojen päivityssykli

Domain name: TADD.LOCAL

DNS Server Zone

| ZONENAME | ZONETYPE | ISAUTOCREATED | ISDSINTEGRATED | ISREVERSELOOKUPZONE | ISSIGNED |
|-------------------|----------|---------------|----------------|---------------------|----------|
| _msdcs.TADD.local | Primary | False | True | False | False |
| 0.in-addr.arpa | Primary | True | False | True | False |
| 127.in-addr.arpa | Primary | True | False | True | False |
| 255.in-addr.arpa | Primary | True | False | True | False |
| TADD.local | Primary | False | True | False | False |
| TrustAnchors | Primary | False | True | False | False |

DNS Server Zone Aging

| ZONENAME | AGINGENABLED | AVAILFORSCAVENGETIME | REFRESHINTERVAL | NOREFRESHINTERVAL | SCAVENGESERVERS |
|------------|--------------|----------------------|-----------------|-------------------|-----------------|
| TADD.LOCAL | False | | 7.00:00:00 | 7.00:00:00 | |

DNS Server Scavenging

| NOREFRESHINTERVAL | REFRESHINTERVAL | SCAVENGINGINTERVAL | SCAVENGINGSTATE | LASTSCAVENGETIME |
|-------------------|-----------------|--------------------|-----------------|------------------|
| 7.00:00:00 | 7.00:00:00 | 00:00:00 | False | |

KUVA 11. Esimerkki toimialueen DNS perustietojen raportista.

Dokumentoimalla DNS-alueet voimme varmistaa, ettei järjestelmästä löydy vanhentuneita tai ylimääräisiä alue määrittäjiä. Ylimääräiset DNS-alue määrittäjät saattavat hidastaa tai haitata sovelusten.

5.3.3 Aktiivihakemisto ja tietoturva

Kuten tutkimuksessa osoitettiin, oli tärkeää, että seurataan tiettyjen ryhmien jäsenyyksiä ja muita perusasetuksia rakenteesta ja tietoturvaan liittyviä asetuksia. Toimialueen hallintaryhmän jäsenyydet oli harkittava hyvin tarkasti. Toimialueen hallintatunnuksella oli oikeudet jokaiseen toimialueeseen kuuluvaan palvelimeen sekä työasemaan, mikäli kirjautumista ei oltu erikseen estetty. Dokumentaation esimerkissä kiinnitetään huomiota seuraaviin hallintatunnuksiin:

Enterprise Admins:

Lumene

Domain Admins:

Lumene
adtest

Schema name:

Lumene

KUVA 12. Esimerkki testi toimialueen järjestelmätason tunnuksien dokumentaatiosta

6 YHTEENVETO JA SAAVUTETUT OMINAISUUDET

Oppinäytetyössä onnistuttiin luomaan dokumentaatio-sovellus, joka hakee aktiivihakemistosta ja siihen integroiduista komponenteista haluttuja tietoa. Sovellus tulosti HTML-formaatissa ulostulon toteutuksessa mainitut osa-alueet.

Sovellus oli julkaistu alustavasti henkilökohtaiseen GitHub-repositorioon. Repositoriosta löytyy ReadMe.md-tiedosto, jossa on ohjeet sovelluksen käyttämiseen.

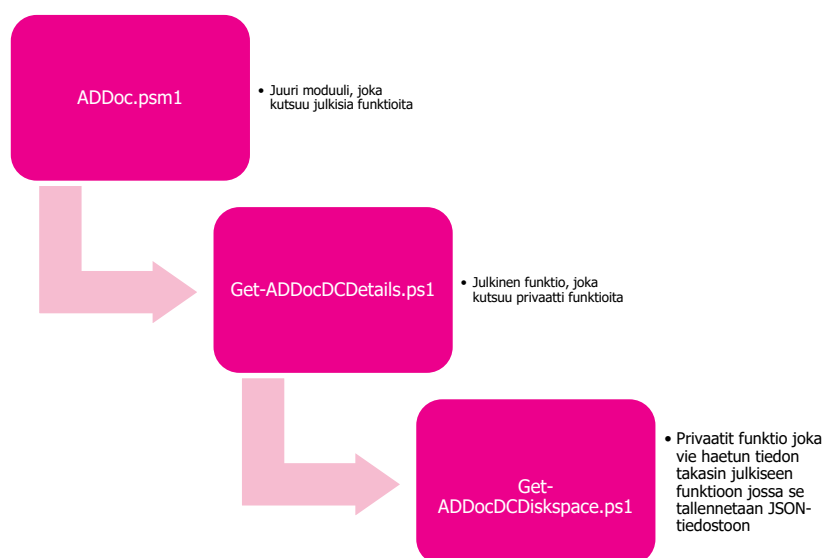
Oppinäytetyössä kehitettiin yleistä tietoturvatietoisuutta, kuten mahdollisten riskien havainnointia ja niiden hallinnointia. Selvityksessä ilmeni, että kaikki IT-ympäristöön liitetyt palvelut ja komponentit, työasemista web-sovelluksiin, voivat heikentää organisaation kokonaistietoturvaa. Siksi on tärkeää seurata ja koordinoita jokaisen IT-palvelun tietoturvariskejä. Tänä päivänä suurimpien riskien joukkoon kuuluu organisaatioiden julkisessa verkossa näkyvät palvelut.

Oppinäytetyössä pääsin tutustumaan ja rakentamaan syvällisempää ajatusmaailmaa ICT-ympäristöstä ja varsinkin aktiivihakemistosta ja sen tietoturva toimenpiteistä. Työn aikana opin tärkeitä tiedonhakutaitoja, joiden avulla löysin myös tärkeitä tietoartikkeleita oppinäytetyöhön liittyen.

Toteutuksen aikana opettelin myös käyttämään PowerShell-skriptausrajapintaa, jonka käyttöä tulevaisuudessa tulen varmasti tarvitsemaan.

6.1 Jatkokehitys

Tarkoituksena on laajentaa dokumentoitavia osa-alueita sekä mahdollisesti uudelleen ohjelmoida datan keruu osio C#-ohjelmointikielellä. Alla kuvataan alkuperäistä ideaa moduulin rungosta, joka osoittautui tarpeettomaksi.



KUVA 7. Alkuperäinen idea moduulin ajatusrungosta.

LÄHTEET

- ATT&CK. (17. Lokakuu 2018). *Initial Access*. Haettu 17. marraskuu 2020 osoitteesta ATT&CK: <https://attack.mitre.org/versions/v8/tactics/TA0001/>
- Berg, L. (5. Kesäkuu 2019). *What is DCSync*. Haettu 18. marraskuu 2020 osoitteesta Stealthbits: <https://stealthbits.com/blog/what-is-dcsync-an-introduction/>
- Commission, F. T. (Huhtikuu 2019). *How to Recognize and Avoid Phishing Scams*. Haettu 13. marraskuu 2020 osoitteesta Federal Trade Commission: <https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>
- Frame, W. (24. Heinäkuu 2016). *Building a PowerShell Module*. Haettu 7. marraskuu 2020 osoitteesta Github: <http://ramblingcookiemonster.github.io/Building-A-PowerShell-Module/>
- Grimes, R. (19. Lokakuu 2010). *How advanced persistent threats bypass your network security*. Haettu 18. marraskuu 2020 osoitteesta CSO Online: <https://www.csoonline.com/article/2624505/how-advanced-persistent-threats-bypass-your-network-security.html>
- Hasayen, A. (13. Maaliskuu 2019). *What is pass the hash attack and how to mitigate it*. Haettu 12. marraskuu 2020 osoitteesta Blog Ahasayen: <https://blog.ahasayen.com/pass-the-hash/>
- Loos, A. (25. Helmikuu 2019). *AD Health & Security Check-up*. Haettu 12. marraskuu 2020 osoitteesta Arnaud Loos: <https://arnaudloos.com/AD-Health-Check/>
- Mera, T. (22. Syyskuu 2020). *Top 4 Active Directory Security Issues from 2 Years of Security Assessments*. Haettu 14. marraskuu 2020 osoitteesta Microsoft Ignite: <https://myignite.microsoft.com/sessions/9d1d586c-ae54-470b-a1d8-820a05258250>
- Metcalf, S. (25. Syyskuu 2015). *Sneaky Active Directory Persistence #13: DSRM Persistence v2*. Haettu 17. marraskuu 2020 osoitteesta Adsecurity: <https://adsecurity.org/?p=1785>
- Metcalf, S. (14. Lokakuu 2015). *The Most Common Active Directory Security Issues and What You Can Do to Fix Them*. Haettu 16. marraskuu 2020 osoitteesta Active Directory Security: <https://adsecurity.org/?p=1684>
- Microsoft. (19. Marraskuu 2014). *Active Directory Collection*. Haettu 2. marraskuu 2020 osoitteesta Docs Microsoft: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780036\(v=ws.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780036(v=ws.10)?redirectedfrom=MSDN)
- Microsoft. (31. Toukokuu 2017). *Active Directory Domain Services Overview*. Haettu 2. marraskuu 2020 osoitteesta Microsoft Docs: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
- Microsoft. (14. Helmikuu 2019). *Active Directory Administrative tier model*. Haettu 7. marraskuu 2020 osoitteesta Microsoft Docs: <https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material>

- Microsoft. (9. Elokuu 2019). *Active Directory Forest Recovery Guide*. Haettu 5. marraskuu 2020 osoitteesta Docs Microsoft: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-guide>
- Microsoft. (21. Marraskuu 2019). *Microsoft Documentation*. Haettu 2. marraskuu 2020 osoitteesta How to Write a PowerShell Script Module: <https://docs.microsoft.com/en-us/powershell/scripting/developer/module/how-to-write-a-powershell-script-module?view=powershell-7.1>
- Petters, J. (29. Maaliskuu 2020). *Kerberos Attack: How to Stop Golden Tickets?* Haettu 14. marraskuu 2020 osoitteesta Varonis: <https://www.varonis.com/blog/kerberos-how-to-stop-golden-tickets/>
- Petters, J. (29. Maaliskuu 2020). *Kerberos Attack: Silver Ticket Edition*. Haettu 14. marraskuu 2020 osoitteesta Varonis: <https://www.varonis.com/blog/kerberos-attack-silver-ticket/>
- Sarode, A. (9. Marraskuu 2020). *Active Directory Attacks -Red It Out*. Haettu 13. marraskuu 2020 osoitteesta Packetstormsecurity.net: <https://dl.packetstormsecurity.net/papers/general/red-it-out.pdf>
- Semperis. (2020. Elokuu 2020). *Recovering Active Directory from Cyber Disasters A SURVEY OF IDENTITY-CENTRIC SECURITY LEADERS*. Haettu 14 marraskuu osoitteesta Semperis: <https://www.semperis.com/wp-content/uploads/2020/08/Recovering-AD-from-Cyber-Attack.pdf>
- Swedin, P. (2014, Lokakuu 23). *Golden ticket, pass the ticket mi tm kerberos attacks explained*. Retrieved marraskuu 2020, from Slideshare: <https://www.slideshare.net/peterswedin/golden-ticket-pass-the-ticket-mi-tm-kerberos-attacks-explained>
- Swinhoe, D. (9. Lokakuu 2019). *Rebuilding after NotPetya: How Maersk moved forward*. Haettu 4. marraskuu 2020 osoitteesta CSO online: <https://www.csoonline.com/article/3444620/rebuilding-after-notpetya-how-maersk-moved-forward.html>