Opinnäytetyö AMK

Tieto- ja viestintätekniikka

2025

Elias Eerola

Kyberturvallisuuden haavoittuvuuksien hallintajärjestelmän suunnittelu ja opas käyttöönottoon konesaliympäristössä

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö AMK Tiivistelmä

Turun ammattikorkeakoulu

Tieto- ja viestintätekniikka

2025 | Sivumäärä 32 + 22 liitesivua

Elias Eerola

Kyberturvallisuuden haavoittuvuuksien hallintajärjestelmän suunnittelu ja opas käyttöönottoon konesaliympäristössä

Yrityksien tietojärjestelmät ovat entistä enemmän keskitettyinä konesaleihin, joiden toiminta on välttämätöntä ja kriittistä konesalien asiakkaille. Kyberturvallisuuden haavoittuvuuksien hallinta on keskeinen haaste konesaleissa, joissa on suuri määrä palvelimia ja lukuisia tietoverkkoja samassa tilassa. Konesaleissa laitteiden hallinnan on oltava mahdollisimman sujuvaa ja helppoa konesalin ylläpitäjille.

Tämän opinnäytetyön tavoitteena oli suunnitella ja ottaa käyttöön keskitetty haavoittuvuuksien hallintajärjestelmä, joka tekee haavoittuvuuksien hallinnasta helppoa luotettavalla ja tehokkaalla tavalla.

Opinnäytetyössä käytiin läpi hallintajärjestelmän kokonaisvaltainen käyttöönotto hallitussa testiympäristössä, joka muistuttaa pientä konesaliympäristöä rakenteellisesti. Validointimenetelmien avulla työssä tarkasteltiin haavoittuvuuksien kriittisyyttä eettisen hakkerin näkökulmasta ja käsiteltiin tyyppilisiä korjaus- ja kovennustoimenpiteitä.

Tuloksena saatiin ohjeistus kokonaisvaltaisen haavoittuvuuksien hallintajärjestelmän käyttöönottoon, jonka avulla haavoittuvuuksia voidaan tarkastella ja hallita yhdestä paikasta.

Asiasanat:

Kyberturvallisuus, haavoittuvuus, tietoturva, palvelinkeskukset

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Information and Communications Technology

2025 | Total number of pages 32 + 22 pages of attachment

Elias Eerola

Cybersecurity Vulnerability Management System Design and Deployment Guide in a Data Center Environment

Companies' information systems are increasingly centralized in data centers, whose operations are essential and critical for the data center customers. The topic raises the question of managing cybersecurity vulnerabilities in the data center environment, when there are large numbers of servers in the same space and numerous data networks. In a critical environment, device management must be as smooth and easy as possible for data center administrators.

This thesis designs and implements a centralized vulnerability management system. Implementation includes design, installation and maintenance measures. The goal is to make vulnerability management easy in a reliable and efficient manner.

This thesis discusses the comprehensive implementation of the management system in a controlled test environment, which structurally resembles a small data center environment. Using validation methods, the work examines the criticality of vulnerabilities from the perspective of an ethical hacker and discusses typical repair and hardening measures.

The end result is a user guide for a comprehensive vulnerability management system that allows you to view and manage vulnerabilities from one place.

Keywords:

cybersecurity, vulnerability, information security, data centers.

Sisältö

Käytetyt lyhenteet tai sanasto **6**

1 Johdanto **7**

2 Haavoittuvuuksien hallinnan perusteet **9**
2.1 Keskeiset käsitteet ja termit 9
2.2 NIS2-direktiivi ja standardit 9

3 Hallintajärjestelmän suunnittelu **12**
3.1 Yleisimmät haavoittuvuudet 12
3.2 Ympäristö ja komponentit 12
3.3 Haasteet suunnittelussa 13

4 Käyttöönotto testiympäristössä ja käyttöoppaan laatiminen **15**
4.1 Käyttöönotto 15
4.2 Asennus ja konfigurointi 17
4.3 Testaus ja validointi 18
4.4 Ylläpitäminen 21
4.5 Päivittäminen 21
4.6 Vianmääritykset 22

5 Tulokset **24**
5.1 Havainnot 24
5.2 Käyttöönoton riskit 24
5.3 Käyttöönoton haasteet 25
5.4 Johtopäätökset ja suositukset 25
5.5 Testitulokset ja analyysit 26

6 Yhteenveto **29**

Lähteet **30**

Liitteet

Liite 1. Hallintajärjestelmän asennusohje
Liite 2. Hallintajärjestelmän käyttäminen ja pentestaus

Kuvat

Kuva 1. Testiympäristön lohkokaavio. 15
Kuva 2. Testiympäristön palomuurin verkkoasetukset. 16
Kuva 3. Rakennettu fyysinen testiympäristö. 16
Kuva 4. Hallintajärjestelmän näkymä kaikista päätelaitteista. 18
Kuva 5. Meterpreter-työkalun käyttäminen. 20
Kuva 6. Hallintajärjestelmän päivittäminen. 22
Kuva 7. Vianmääritys palvelut-välilehdellä Windows Server-palvelimella. 23
Kuva 8. Vianmääritys lokitiedostoista Windows Server-palvelimella. 23
Kuva 9. Rapid7-hallintajärjestelmän yleiskuva päätelaitteista. 26
Kuva 10. Rapid7-hallintajärjestelmän yleiskuva päätelaitteiden haavoittuvuuksien riskipitoisuudesta. 27
Kuva 11. Lista löydetyistä haavoittuvuuksista päätelaitteella. 27

Käytetyt lyhenteet tai sanasto

CVE	Common vulnerabilities and exposures, yleisiä haavoittuvuuksia ja altistumisia
GB	Gigabitti
HYPER-V	Windowsin virtualisointitekniikka
IP	Internet protokolla
ISO	International organization for standardization
LAN	Local area network, sisäverkko
METASPLOIT	Penetraatiotestaustyökalu
METERPRETER	Penetraatiotestaustyökalu
NAT	Network address translation, verkko-osoitteen käännös
NIS2	Network and information security 2, verkko- ja tietoturva 2
NMAP	Penetraatiotestaustyökalu
PENTESTAUS	Penetraatiotestaus
VPN	Virtual private network, virtuaalinen yksityinen verkko
VLAN	Virtuaalinen verkko
WAN	Wide area network, ulkoverkko

1 Johdanto

Tämän opinnäytetyön aiheena on kyberturvallisuuden haavoittuvuuksien hallintajärjestelmän suunnittelu ja opas käyttöönottoon konesaliympäristössä toteutettuna kotimaiselle ICT-palveluntarjoajalle. Tässä opinnäytetyössä käsitellään, kuinka haavoittuvuuksia voidaan hallita teknisellä tasolla palvelinympäristössä.

Konesaleissa ylläpidetään palvelimia, joissa yrityksien kriittiset palvelut toimivat. Tämän vuoksi konesaliympäristöt ovat erittäin kriittisiä tietoturvan suhteen. Konesalitoimittajien ja yrityksen IT-vastaavien on suunniteltava tarkkaan oikeat ratkaisut tietoturvan ja kyberturvallisuuden osalta. Ilman kunnollista haavoittuvuuksien hallintaa, konesalin palvelimien haavoittuvuuksia on vaikea tunnistaa, analysoida ja korjata. Tämä altistaa konesalin palvelimet erilaisille kyberhyökkäyksille.

Tämän opinnäytetyön tavoitteena on rakentaa kokonaisvaltainen haavoittuvuuksien hallintajärjestelmä konesaliympäristöön käyttöoppaan muodossa. Yritystoiminta on nykyään hyvin riippuvainen tietojärjestelmistä ja niiden sujuvasta toiminnasta, joka tekee aiheesta tärkeän ja ajankohtaisen. Yrityksillä on edelleen haasteita haavoittuvuuksien hallintajärjestelmän toteutuksessa. Yrityksien tietoisuus haavoittuvuuksista on edelleen melko vähäistä ja usein tietoturvatoimissa keskitytään vain suojaamaan perustasolla laitteet. Roytman ja Bellis (2023, 3, 8, 188) kuvaavat näitä haasteita ja sitä, kuinka tärkeää yrityksille on kyberturvallisuusriskien aktiivinen kartoitus.

Opinnäytetyössä keskitytään haavoittuvuuksien hallintaan ja sen sisällyttämiseen osaksi yrityksen arkea teknisesti ja otetaan huomioon myös nykyiset direktiivit ja standardit.

Hallintajärjestelmän tarkoituksena on olla ratkaisu, joka edistää haavoittuvuuksien tunnistamista ja palvelimien koventamista nopeasti kehittyvän teknologian mukana. Opinnäytetyössä käsitellään myös

haavoittuvuuksia yleisesti ja sitä, miten esimerkiksi NIS2-direktiivi suhtautuu haavoittuvuuksiin.

Opinnäytetöitä samankaltaisesta aiheesta löytyi yksittäisiä. Aihetta on käsitelty monesta eri perspektiivistä. Täysin samasta aiheesta, joka käsittelisi haavoittuvuuksien hallintaa konesaliympäristössä, ei löytynyt.

ISO/IEC 27000 -standardisarja tarjoaa suosituksia tietoturvallisuuden hallintaan riskien vähentämiseen ja kontrollointiin (ISO/IEC 27000). Laulaisen (2024) opinnäytetyössä todetaan, että ISO/IEC 27000 -standardisarjan suositusten avulla yrityksen on mahdollista toteuttaa tietoturvan hallintajärjestelmä organisaatiossa, oppia parhaimmista käytännöistä ja valmistautua tietoturvaan liittyviin auditointeihin. Standardisarja on suunniteltu kaikenkokoisille yrityksille.

Laulaisen (2024) työssä käsitellään myös kyberturvallisuuden haavoittuvuuksia. Lainatussa kappaleessa käsitellään yrityksen tietoturvan hallintaan liittyviä standardeja. Viitatun opinnäytetyön käsittelemien tietoturvastandardien lisäksi osalla yrityksistä on velvollisuus noudattaa NIS2-direktiiviä.

Virkkulan (2023) opinnäytetyössä käsitellään kyberturvallisuutta eettisen hakkerin silmin. Siinä käsitellään penetraatiotestaukseen käytettäviä sovelluksia, erityisesti Nmap-työkalua, jonka avulla on mahdollista etsiä tietoverkoista avoimia portteja. Nmap on edelleenkin tehokas työkalu verkkojen tutkimiseen. Kyseistä työkalua on myös hyödynnetty tässä opinnäytetyössä.

Ruottisen (2023) opinnäytetyössä tutkitaan haavoittuvuusskannerin käyttämistä kohdeyrityksessä. Tutkimuksessa käytetyn haavoittuvuusskannerin valinnassa korostui skannerin sopivat ominaisuudet, käyttökustannukset ja helppokäyttöisyys.

2 Haavoittuvuuksien hallinnan perusteet

2.1 Keskeiset käsitteet ja termit

Kyberturvallisuudessa haavoittuvuus on yleinen termi, jota käytetään kuvastamaan heikkouksia esimerkiksi tietojärjestelmissä, laitteissa ja ohjelmissa (Tepa-termipankki 2023). Haavoittuvuus kuvastaa heikkoutta, jota kyberhyökkääjä voi käyttää tietojärjestelmään tunkeutumisessa. Kun ohjelmassa, tietojärjestelmässä tai laitteessa on aukko, se on silloin haavoittuvainen.

Tietoturva-asiantuntijat etsivät haavoittuvuuksia järjestelmällisesti, jonka pohjalta haavoittuvuuksia korjataan. Periaatteessa sellaista järjestelmää ei ole olemassa, joka ei olisi millään tavalla haavoittuvainen. On vain haavoittuvuuksia, joita on tunnistettu ja joita ei ole vielä tunnistettu. Siksi jatkuva haavoittuvuuksien etsiminen on erittäin tärkeää.

2.2 NIS2-direktiivi ja standardit

NIS2-direktiivi on uusi Euroopan unionin laatima kyberturvallisuusdirektiivi, jonka tarkoitus on parantaa kyberturvallisuutta yhtenäisesti koko Euroopan unionissa (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555).

Ennen NIS2-direktiiviä tietoturvaa on pääasiassa hallittu maakohtaisesti kyberturvallisuuslailla. Tämä on aiheuttanut sen, että yrityksien välillä on suuria eroja kyberturvallisuuden ja tietoturvan toteutuksessa (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, johdanto-osan kappale 4). Tämä näyttää johtaneen tilanteeseen, jossa joissain yrityksissä aihe on ollut tärkeyslistalla ensimmäisenä ja toisinaan se on jätetty liian vähäiselle huomiolle. Monissa yrityksissä on saattanut olla vahva usko siihen, että ”kyllä kaikki on kunnossa”. Todellisuudessa kyberturvallisuuden maailmassa ei voida olla koskaan tilanteessa, jossa voidaan olettaa, että kaikki on kunnossa. Kyberturvallisuudessa kehitys on oltava jatkuvaa ja pysähtymätöntä. Tämän lisäksi ajattelun tulee olla nollaluotto-mallinen. NIS2-direktiivin tehtävä on nimenomaan kääntää ajattelutapa tähän suuntaan. Ilman direktiiviä olisi

edelleen liian suuria eroja yrityksien tietoturvan ja kyberturvallisuuden toteutuksessa.

Direktiivi on lista vaatimuksista, joita yrityksen tulee noudattaa, mikäli yritys kuuluu NIS2-direktiivin soveltamisen piiriin. Tämä määritetään sen mukaan minkä kokoinen yritys on henkilöstöltään, liikevaihdoltaan ja millä sektorilla yritys toimii (Traficom 2024).

Direktiivi ei siten koske kaikkia yrityksiä. Se koskettaa pääasiassa kriittisellä sektorilla toimivia yrityksiä ja suuremman kokoluokan yrityksiä. Esimerkiksi suomalaisille toimijoille materiaalia valmistava pk-yritys, jonka liikevaihto on 1–2 miljoonaa euroa vuodessa ja henkilöstö 30 henkilöä, ei kuulu NIS2-direktiivin piiriin alhaisen liikevaihdon ja henkilöstön määrän vuoksi (Traficom 2024).

Traficom (2024) on julkaissut taulukon, joka osoittaa miten direktiiviä sovelletaan erialoilla toimiviin yrityksiin ja suhteessa niiden kokoon. Taulukon mukaan erittäin kriittiset toimialat, kuten energia-, liikenne-, pankki-, juoma- ja jätevesilaitokset sekä tieto- ja viestintätekniikan palveluiden hallinta kuuluvat direktiivin soveltamisalaan käytännössä välittömästi.

Direktiivi asettaa erilaisia velvoitteita yrityksen kyberturvallisuuden ja tietoturvan suhteen. Yrityksellä tulee olla käytössä kattava riskienhallintajärjestelmä, jonka ytimessä on riskienarviointi. Yrityksellä on oltava siis järjestelmä, johon kirjataan löydetyt riskit ja niiden korjaustoimenpiteet.

Yrityksellä on kolmivaiheinen ilmoitusvelvollisuus tietoturvapoikkeamissa. Ilmoitusvelvollisuus on määritetty ajallisesti.

Haavoittuvuuksien hallinta on olennainen ja kriittinen osa NIS2-direktiiviä, jonka vuoksi tässä opinnäytetyössä käydään läpi myös NIS2-direktiivin vaatimuksia. Yrityksellä on oltava kyky ohjelmistojen ja käyttöjärjestelmien haavoittuvuuksien tunnistamiseen ja korjaamiseen. Tässä opinnäytetyössä käytetään Rapid7-järjestelmää, joka on Gartnerin tutkimuslaitoksen asiakaskyselyn mukaan yksi eniten käytetyistä haavoittuvuusskannereista, joka saa myös käyttäjiltä hyvät arvostelupisteet (Gartner 2025). Järjestelmän avulla voidaan tehdä

haavoittuvuuksien tunnistamisesta automaattista. Tämä helpottaa haavoittuvuuksien dokumentointia ja raportointia. Tämän lisäksi korjaustoimenpiteet voidaan helposti suorittaa tiimityöskentelynä esimerkiksi tietoteknisen tiimin kanssa.

Riskienhallinta on jatkuva prosessi ja yrityksen on luotava ratkaisu tämän prosessin ylläpitämiseksi, jotta se voi täyttää direktiivin vaatimukset.

Kun yritys toteuttaa ja vahvistaa tietoturvaa, voi yritys tukeutua tietoturvaan liittyviin standardeihin. Osittain standardien noudattaminen IT-alalla voi olla myös pakollista tai velvoite sen noudattamiseen voi tulla sidosryhmien kautta (Yli-Hietanen K. 2021).

Aikaisemmin käsitelty NIS2-direktiivi sisältää vaatimuksissaan paljon samanlaisia asioita kuin esimerkiksi ISO 27001 -standardi (ISO 2022), jota käytetään lähtökohtaisesti yrityksen tietoturvanhallintajärjestelmän rakentamisessa. Tietoturvahallintajärjestelmä kuuluu yrityshallinnon ydintoimintoihin. Hallintajärjestelmä sisältää esimerkiksi tietoturvapolitiikat, riskienhallinnan, tietoturvaloukkausten hallintasuunnitelman ja esimerkiksi päätelaitteiden yleisen hallinnan. Sen tarkoitus on olla keskitetty paikka hallitakseen yleisesti yrityksen tietoturvallisuutta. Standardia varten yritys rakentaa järjestelmän itse tai hyödyntämällä ulkoisia työkaluja.

Yritys voi hyödyntää ISO 27001 -standardia NIS2-direktiivin vaatimuksien täyttämiseen. Direktiivi on lista vaatimuksista, kun taas standardi toimii oppaana vaatimuksien toteuttamiseen. SFS Suomen Standardit ry on julkaissut suomenkielisen SFS ISO 27001 standardin, joka tukee yrityksen tietoturvallisuutta (SFS-EN ISO 27001. 2023).

3 Hallintajärjestelmän suunnittelu

3.1 Yleisimmät haavoittuvuudet

Haavoittuvuuksia on paljon ja monenlaisia. Yleisimmät haavoittuvuudet liittyvät päivittämättömiin käyttöjärjestelmiin ja ohjelmiin. Esimerkiksi haittaohjelmat aiheuttavat haavoittuvuuksia järjestelmiin. Myös vääränlaiset tai virheelliset käyttöjärjestelmien asetukset ja heikot salausmenetelmät aiheuttavat haavoittuvuuksia. Tämän lisäksi heikot salasanat ovat haavoittuvuuksia. Kaikki asiat, jotka luokitellaan aukoiksi, ovat haavoittuvuuksia (Traficom 2020).

3.2 Ympäristö ja komponentit

Tämän opinnäytetyön ytimessä on hallintajärjestelmän käyttöönottaminen. Ennen hallintajärjestelmän käyttöönottoa on tärkeää vertailla hallintajärjestelmien eroja. Hallintajärjestelmä kannattaa valita yrityksen tarpeen mukaan.

Haavoittuvuuksien hallintajärjestelmä

Haavoittuvuuksien hallintajärjestelmä on yrityksen sisäinen työkalu, jonka avulla etsitään päätelaitteista haavoittuvuuksia, eli aukkoja, joita ulkopuolisten tahojen on mahdollista hyödyntää järjestelmään tunkeutumisessa.

Hallintajärjestelmän tarkoitus ei ole ainoastaan ilmoittaa löydetyistä haavoittuvuuksista, vaan tehdä siitä automaattista ja osa yrityksen rutiinia. Sen tavoite on luoda lisäkerros suojausta yrityksen tietojärjestelmiin, jotta minimoidaan kaikki mahdolliset riskit.

Vaikka hallintajärjestelmän päätehtävänä on etsiä ja raportoida haavoittuvuuksia, sen tärkeä tehtävä on myös auttaa yrityksen IT-osastoa löytämään oikeat ratkaisut niiden korjaamiseksi.

Järjestelmän avulla saadaan myös tärkeää ja säännöllistä dokumentaatiota organisaation haavoittuvuuksista, joita voidaan tarvita esimerkiksi auditoinneissa ja liittyen NIS2-direktiivin raportointivelvollisuuksiin, joissa raportoinnin säännöllisyys on avainasemassa.

Haavoittuvuuksien hallintajärjestelmän tarpeellisuus

Teknologia on kehittynyt siihen pisteeseen, että pelkkä päätelaitteiden suojaus virustorjuntaohjelmilla ja päivityksien ylläpitämisellä ei riitä. Virustorjuntaohjelmat eivät yleensä kerro minkälaisia aukkoja laitteelta löytyy, vaan ilmoittaa vasta kun mahdollinen tunkeutuminen laitteeseen on havaittu tai hyökkääjä on onnistunut asentamaan päätelaitteelle haittaohjelman, jonka avulla voi päästä päätelaitteen hallintaan (Traficom 2022).

Tämä on suuri ongelma, koska organisaatioissa usein luotetaan ajatukseen, että tietoturva on kunnossa.

NIS2-direktiivin astuttua voimaan on nollaluottoajattelu eli “Zerotrust” tullut vahvaan asemaan kyberturvassa (Elisa 2021). Tämä tarkoittaa sitä, että asioita lähestytään pienimmällä mahdollisella luottamuksella. Esimerkiksi käyttöoikeudet ja organisaation henkilöstön pääsy asetetaan pienimpään asteeseen. Vaikka nollaluottoajattelua noudatettaisiin pääsynhallinnan osalta, niin on yhtäältä tärkeää saavuttaa tarkka ja säännöllinen näkyvyys järjestelmien sisälle. Nollaluottoajattelun mukaan yrityksen ei tulisi koskaan ajatella, että ”tietoturva on kunnossa”. Ilman kunnollista näkyvyyttä järjestelmän sisälle on vaikea tietää, minkälaisia uhkia organisaation laitteille kohdistuu. Todellisuudessa tietoturva ei voi olla koskaan niin kunnossa, että voitaisiin luottaa täysin tietoturvan tasoon, koska uusia uhkia syntyy jatkuvasti, kun uusia tietoteknisiä järjestelmiä keksitään. Haavoittuvuuksien hallintajärjestelmä tulisi siis olla kaikilla organisaatioilla käytössä.

3.3 Haasteet suunnittelussa

Hallintajärjestelmän suunnitteluun kuului fyysisten ratkaisujen valitseminen ja järjestelmien tekninen suunnittelu. Suunnittelussa oli otettava huomioon, että testiympäristö tarvitsee riittävästi suorituskykyä ja että testiympäristön on oltava eristetyssä ja hyvin hallitussa verkossa.

Hallintajärjestelmän suunnittelussa ilmeni haasteita. Testiympäristön rakentamisessa rajoittavana tekijänä oli fyysiset resurssit. Tyypillisiä tilanteita olivat keskusmuistin äkillinen loppuminen tai vähäinen tallennustila.

Yleinen haaste hallintajärjestelmän käyttöönoton suunnittelussa on käyttöönoton varmistaminen. Tämä tarkoittaa prosessia, jossa varmistetaan, että hallintajärjestelmän agentti eli valvontaohjelma on onnistuneesti asennettu kaikille organisaation päätelaitteille.

Pulmatilanteita voi tulla vastaan esimerkiksi hallintajärjestelmän agentin yhteensopivuudessa käyttöjärjestelmien kanssa. Testiympäristön suunnitteluvaiheessa tarkoituksena oli hallintajärjestelmän agentin asentaminen vanhemmalle Windows Server 2012 -palvelimelle, jossa haavoittuvuuksia testikäytössä olisi lähtökohtaisesti ollut enemmän mutta palvelinta ei saatu näkyviin hallintajärjestelmässä, johtuen vanhasta käyttöjärjestelmästä.

Lisäksi hallintajärjestelmän käyttöönoton budjetointi voi olla haasteellista. Päätelaitteiden määrää voi olla vaikeaa suunnitteluvaiheessa arvioida. Päätelaitteiden määrä määrittää yleisesti myös taloudelliset kulut.

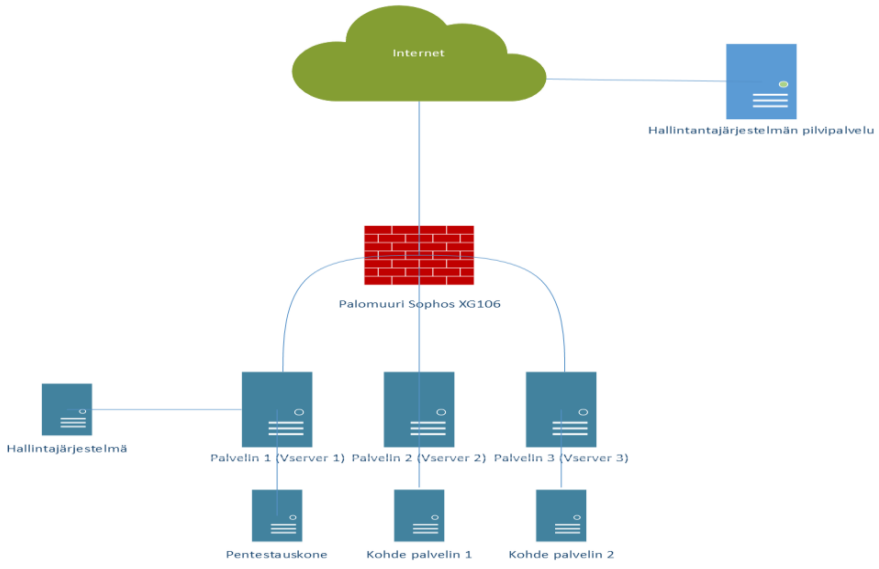
4 Käyttöönotto testiympäristössä ja käyttöoppaan laatiminen

4.1 Käyttöönotto

Tässä opinnäytetyössä pystytettiin kattava testiympäristö, joka muistuttaa konesaliympäristöä. Työskentely aloitettiin valitsemalla riittävät fyysiset resurssit. Ympäristön pystytykseen tarvittiin muutama fyysinen palvelin, palomuurilaite, riittävästi keskusmuistia, levytilaa ja tarvittavat käyttöjärjestelmät.

Testiympäristön pystytys

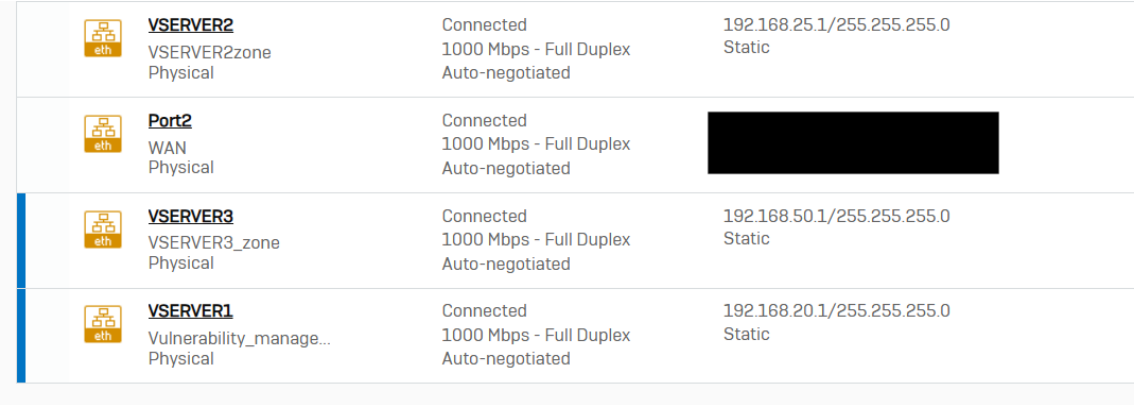
Testiympäristön suunnittelu aloitettiin piirtämällä lohkokaavio mistä rakennettava kokonaisuus selviää (Kuva 1). Tämän jälkeen aloitettiin testiympäristön rakentaminen. Kun laitteet oli järjestetty testiympäristöä varten, asennettiin laitteet.



Kuva 1. Testiympäristön lohkokaavio.

Palvelimille asennettiin Windows Server 2019 -käyttöjärjestelmät. Palomuuriksi asennettiin Sophos XG 106, jossa on 3 paikkaa päätelaitteille ja yksi paikka internet-yhteydelle (wan) (Kuva 2). Tässä tilanteessa ei tarvittu kytkintä, koska

paikkoja palomuurissa oli riittävästi. Fyysiset palvelimet kiinnitettiin palomuuriin, josta jokaiseen menee oma verkko. Jokaiselle palvelimelle menevän verkon mukana kuljetettiin myös virtuaaliverkot virtuaalipalvelimia varten.



Kuva 2. Testiympäristön palomuurin verkkoasetukset.

Tässä vaiheessa fyysinen ympäristö oli rakennettu (Kuva 3). Palvelimet voitiin nyt käynnistää. Fyysiset palvelimet toimivat tässä tilanteessa isäntäpalvelimina eli palvelimina, jotka virtualisoivat muita palvelimia. Kaikki palvelimet virtualisoitiin isäntäpalvelimille käyttäen Microsoftin Hyper-V-teknologiaa.

Kuva 3. Rakennettu fyysinen testiympäristö.

Loin ensimmäisen virtuaalipalvelimen Hyper-V-ympäristöön, jossa Rapid7-komentokeskus tulee toimimaan. Tämä virtuaalipalvelin tarvitsee keskusmuistia ja suorituskykyä enemmän kuin muut palvelimet, jotta varmistamme hallintajärjestelmän toiminnan ongelmitta.

4.2 Asennus ja konfigurointi

Työssä asennettiin ja käytettiin Rapid7 Insightvm-nimistä hallintajärjestelmää (Rapid7 2025a). Kyseessä on hallintajärjestelmän toimittajan Rapid7-tuote.

Hallintajärjestelmän asennus on oleellinen osa kokonaista käyttöönotto prosessia. Liitteessä 1 on kuvattu hallintajärjestelmän asennus testiympäristöön ja päätelaitteille vaiheittain. Hallintajärjestelmän asennus koostuu hallintajärjestelmän moottorin asentamisesta ja agenttien asentamisesta päätelaitteille. Moottori toimii haavoittuvuusskannerina. Päätelaitteille asennetut agentit etsivät haavoittuvuuksia ja välittävät tiedot moottorille pilvipalvelun kautta.

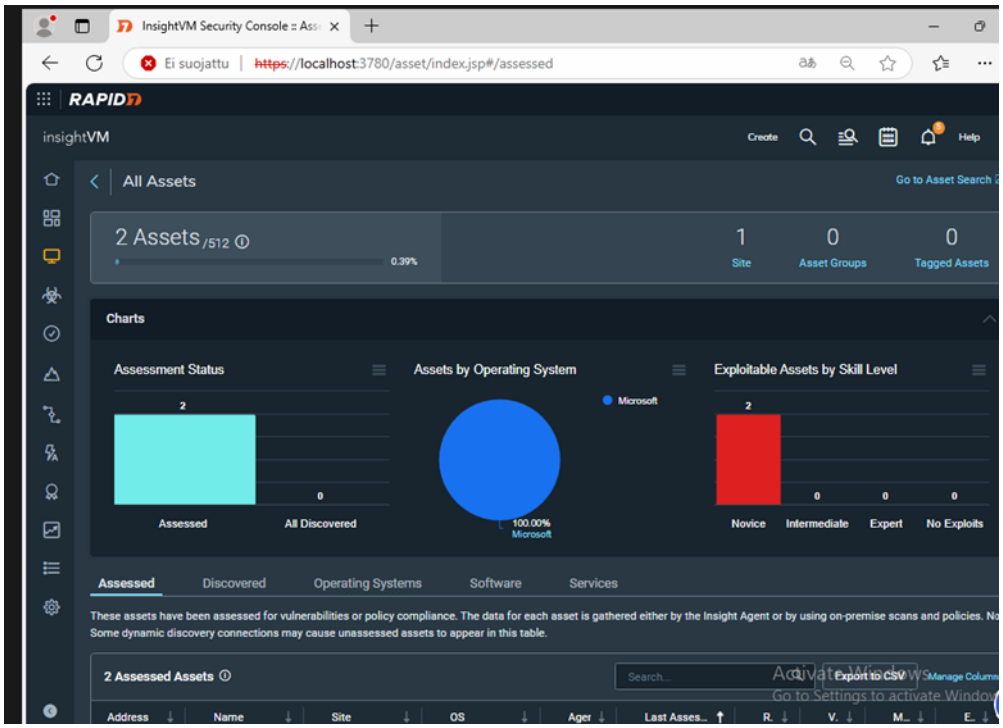
Testiympäristö jäljittelee konesaliympäristöä, jonka vuoksi asennus on suunniteltava huolellisesti. Ennen asennusta on tärkeää huomioida, kuinka verkko toteutetaan, kuten liitteessä 1 kerrotaan. Liitteen ohjeessa on myös esimerkki, kuinka verkko on rakennettu käyttäen fyysistä palomuurilaitetta. Erityisesti on huomioitava, että hallintajärjestelmä asennetaan omaan eristettyyn verkkoon ja omalle erilliselle palvelimelleen.

Hallintajärjestelmä asennetaan palvelimelle käyttäen asennuspakettia, joka tulee tuotteen mukana. Asennuksen jälkeen hallintakeskus on avattavissa paikallisesti palvelimella, josta järjestelmää käytetään. Ohjeen mukaisesti hallintajärjestelmän pilvipalveluliitos mahdollistaa järjestelmän käyttämisen turvallisesti myös internetin kautta, joka tekee käytöstä käytännöllisempää.

Oppaassa käydään läpi päätelaitteiden lisääminen järjestelmään. Päätelaitteille luodaan oma agentti, joka valvoo päätelaitetta. Agentti asennetaan

pilvihallintapaneelista sopivalle käyttöjärjestelmälle, minkä jälkeen päätelaite tulee hallittavaksi järjestelmään.

Hallintajärjestelmän asennusvaiheiden jälkeen, järjestelmä on käytettävissä hallintapaneelin kautta. Hallintapaneelin kautta (Kuva 4) nähdään päätelaitteiden yleinen tila ja laitteiden määrä ympäristössä.



Kuva 4. Hallintajärjestelmän näkymä kaikista päätelaitteista.

4.3 Testaus ja validointi

Pentestaus yleisesti

Penetraatiotestauksella tarkoitetaan menettelytapaa, jossa ammattilainen, kuten ulkopuolinen toimija tai valkohattuhakkeri yrittää murtautua yrityksen tietojärjestelmiin käyttäen hakkereiden työkaluja (VPN Unlimited 2025a). Pentestaus on käyttökelpoinen tilanteessa, jossa organisaatiossa halutaan selvittää todellinen puolustuskyky ja varmistaa suojausmenetelmien toimintakyky hyökkäystilanteessa (Blackduck 2025). Pentestaus tarkoittaa

toimintamallia, jossa tunkeutujalla, kuten eettisellä hakkerilla on lupa etsiä keinoja ja yrittää tunkeutua tietojärjestelmiin organisaatiossa. Tämä on siis täysin luvallinen toimintamalli, kun tekijöillä on siihen lupa organisaatiossa, vaikka siinä käytetään keinoja, joita käytetään myös pahatahtoisessa hakkeroinnissa. Tietojärjestelmien ylläpidosta vastaavalle henkilöstölle ei välttämättä ole kerrottu pentestauksesta (Broad & Bindner 2013, 227).

Pentestaus on keino, joka mahdollistaa todellisen hyökkäysrajapinnan testaamisen ja analysoinnin organisaatiolle. Ilman pentestausta ei ole täyttä varmuutta minkälainen hyökkäysrajapinta organisaatiolla on vaikka olisikin hyvät suojausmenetelmät käytössä.

Kali Linuxin asentaminen

Pentestaukseen käytettäviä työkaluja on saatavilla yksittäisesti, mutta Kali Linux mahdollistaa kaikkien tärkeimpien työkalujen käyttämisen yhdestä paikasta. Garnin mukaan (2025) KaliLinux on maailman käytetyimpiä pentestaukseen käytettäviä käyttöjärjestelmiä. Käyttöjärjestelmä asennetaan virallisilta sivuilta. Asennusmuotoja on saatavilla useita ja asennamme tässä tilanteessa Kali Linuxin virtuaalikoneena testiympäristön yhdelle isäntäpalvelimelle.

Virtuaalikoneelle on suositeltavaa antaa riittävästi keskusmuistia ja tallennustilaa. Sen suorituskyky riippuu täysin sen käytettävissä olevista resursseista.

Tässä testiympäristössä Kali Linuxilla on 4 GB keskusmuistia ja noin 100 GB tallennustilaa.

Tärkeimmät työkalut

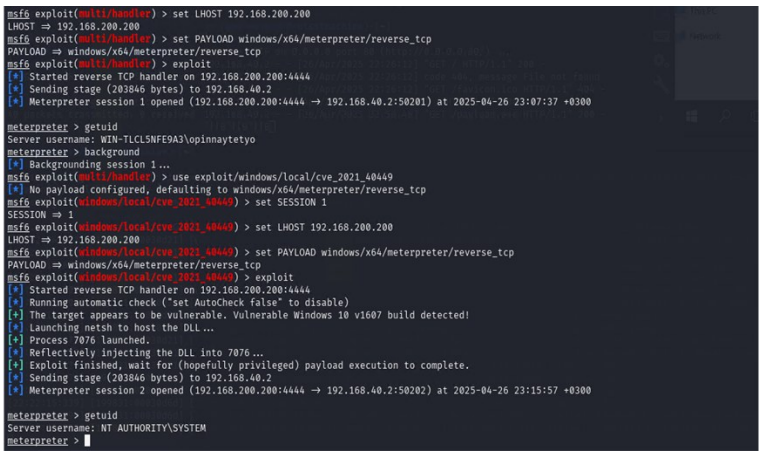
Kali Linuxissa on kattava määrä työkaluja pentestaukseen. Näistä tärkeimpiä ovat Nmap ja Metasploit. Nämä ovat tyypilliset työkalut alkuvaiheeseen, kun ympäristöön yritetään tutustua tarkemmin. Nmapilla etsitään tyypillisesti avoimet portit ja palvelut. Metasploitilla etsitään haavoittuvuuksia.

Kokonaissuoritus ja validointi Kali Linuxilla

Hallintajärjestelmästä voidaan tarkastella päätelaitteita yksityiskohtaisesti. Hallintajärjestelmän toimivuuden varmistamiseksi validointi on tärkeä osa prosessia, jotta haavoittuvuuksien olemassaolo varmistetaan ennen haavoittuvuuden korjaamista ja korjauksen jälkeen.

Liitteessä 2 käydään läpi yksityiskohtaisesti validointivaihe käyttäen asennettua hallintajärjestelmää ja pentestaustyökaluja. Validointivaihe alkaa yksityiskohtaisella päätelaitteen tarkastelulla. Hallintajärjestelmästä voidaan ottaa suoraan raportti löydetyistä haavoittuvuuksista. Raportti sisältää lähtökohtaisesti löydetyt haavoittuvuudet ja vaaditut korjaustoimenpiteet. Haavoittuvuudet on listattu kriittisyysasteikon mukaisesti. Yksityiskohtaisessa ohjeessa validoidaan vakava haavoittuvuus ”CVE-2021-40449: Win32k Elevation of Privilege Vulnerability”. Haavoittuvuutta käyttäen hyökkääjällä on mahdollisuus saada pääkäyttäjän oikeudet palvelimelle.

Seuraavassa vaiheessa muodostetaan etäyhteys palvelimelle tavallisella käyttäjällä. Käyttäjä luo tämän jälkeen haavoittuvuuden hyväksikäytön mahdollistavan ohjelman. Ohjelman luomiseen käytetään Metasploit-työkalua ja meterpreter-työkalua, jotka kohdistetaan haavoittuvuuteen. Ohjelma siirretään palvelimelle, jonka jälkeen se avaa kuvan 5 mukaisesti tunkeutujalle pääkäyttäjän oikeudet palvelimen hallintaan pentestauskoneelta.



Kuva 5. Meterpreter-työkalun käyttäminen.

4.4 Ylläpitäminen

Hallintajärjestelmän monipuolisuus nähdään asennuksen jälkeen erityisesti ylläpidollisesti. Liitteessä 2 käydään hallintakeskuksen ylläpidollisia toimenpiteitä. Yksi toiminnoista on hyödyllinen raportointijärjestelmä, jonka avulla voidaan luoda säännöllisiä raportteja haavoittuvuuksista. Ohjeessa käytetään esimerkkinä korjausraporttia, josta nähdään havaitut haavoittuvuudet ja niiden korjaustoimenpiteet.

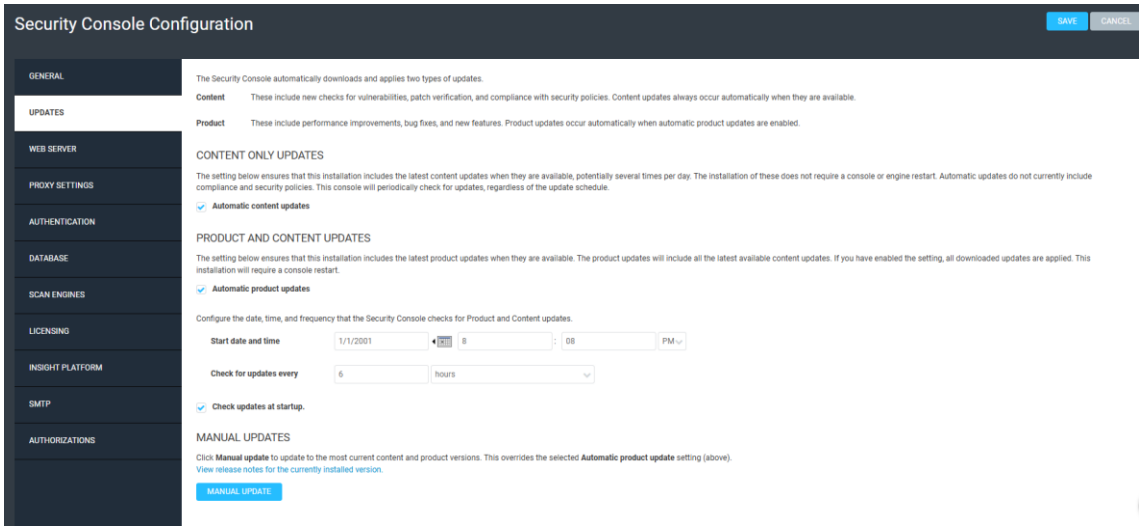
Haavoittuvuuksien korjaaminen

Haavoittuvuuksien tunnistamisen jälkeen, niiden korjaustoimenpiteet voivat sisältää ohjelmistopäivityksiä, järjestelmien asetuksien muuttamista ja lisätoimenpiteitä esimerkiksi ohjelmistotoimittajilta ja tietoturva-asiantuntijoilta. Näillä toimenpiteillä pyritään pienentämään haavoittuvuuksiin liittyviä riskejä ja siten vahvistaa kyberresilienssiä (VPN Unlimited 2025b).

Haavoittuvuuksien korjaaminen on ylläpidollinen toimenpide, jossa löydetty haavoittuvuus korjataan tai palvelinta kovennetaan haavoittuvuuden korjaamiseksi. Kuten liitteessä 2 kerrotaan, haavoittuvuus pyritään korjaamaan kokonaan korjaustoimenpiteillä. Tässä tapauksessa hallintajärjestelmä kertoo tiedon toimenpiteistä, joita ylläpitäjän tulee tehdä.

4.5 Päivittäminen

Hallintajärjestelmän yleinen tehtävä on tarkkailla haavoittuvuuksia päätelaitteilla ja kertoa päivityksistä, joilla yleensä korjataan haavoittuvuuksia. Kuitenkin myös hallintajärjestelmän päivityksistä on yhtä lailla huolehdittava kuin päätelaitteiden päivityksistäkin. Päivityksien asentaminen onnistuu hallintajärjestelmän ylläpitovalikosta asennusohjeen mukaisesti (Kuva 6). Asennusohjeessa korostetaan myös käyttöjärjestelmäpäivityksiä palvelimella, jolle hallintajärjestelmä on asennettu, jotta myös haavoittuvuuksia suljetaan pois palvelimelta.

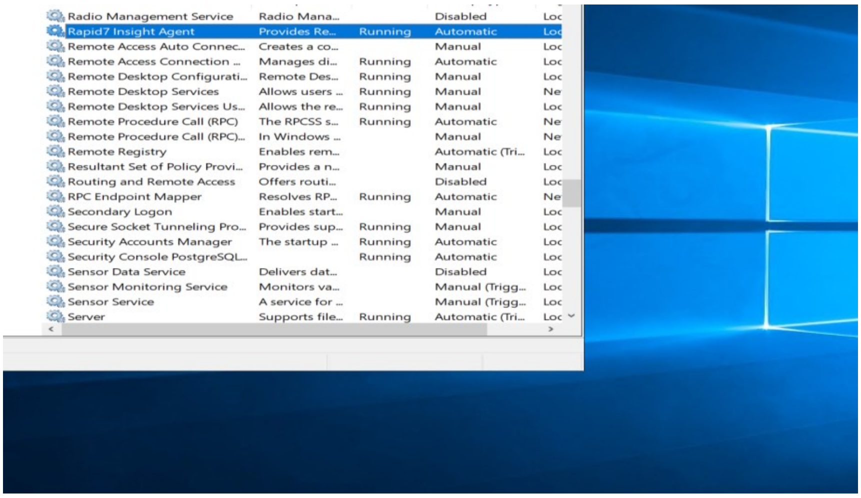


Kuva 6. Hallintajärjestelmän päivittäminen.

4.6 Vianmääritykset

Tilanteissa, joissa Rapid7-hallintajärjestelmässä ilmenee ongelmia, on suositeltavaa ensin tutkia lokitiedostoja ongelmien korjaamiseksi. Lokitiedostot antavat yleistä tietoa hallintajärjestelmän toiminnasta. Niiden tarkasteleminen on myös hyödyllistä hallintajärjestelmän ylläpidon kannalta (Rapid7 2025b).

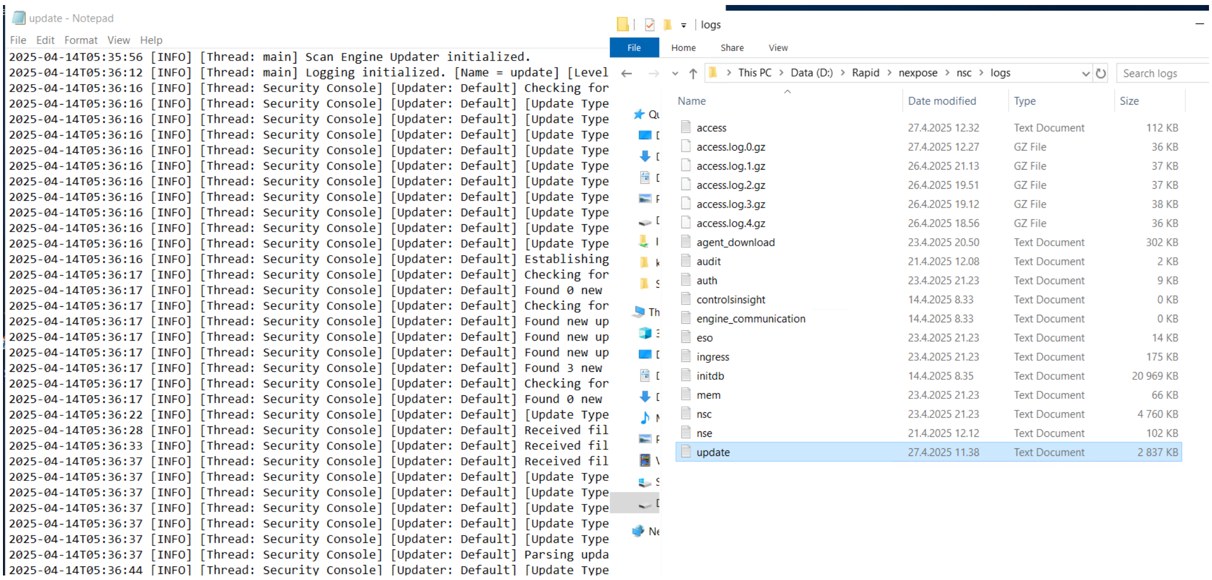
Vaikka hallintajärjestelmä olisi asennettu onnistuneesti, joskus tilanteita voi tulla vastaan, että vianmääritystä tarvitaan ongelman ratkaisemiseksi. IT-järjestelmissä vianmääritys aloitetaan usein lokitiedostojen tarkastelulla ja perusasioiden tarkistuksella (Kuva 7). Viitaten yllä mainittuun lainaukseen, hallintajärjestelmän toimittajan nettisivuilla kerrotaan, että vianmääritys prosessina on hyvä aloittaa selvittämällä lokitiedostoista mihin osioon vika kohdistuu. Tämä on tärkeää tunnistaa koska muuten vianselvitys on haastavaa. Se voi kohdistua esimerkiksi siihen, että hallintajärjestelmä ei aukea tai päätelaitetta ei löydy järjestelmästä. On hyvä tarkistaa, että hallintajärjestelmän palvelu on käynnissä palvelimella. Testiympäristön hallintajärjestelmä on asennettu opinnäytetyötä varten Windows Server 2019 -palvelimelle, joten palvelun tilan voi tarkistaa Windowsin palvelut-välilehdeltä. Kuvasta 7 voidaan päätellä, että palvelu on käynnissä.



Kuva 7. Vianmääritys palvelut-välilehdellä Windows Server-palvelimella.

Rapid7 dokumentaation mukaisesti hallintajärjestelmä kerää lokitietoja sen asennuskansioon. Lokitietojen tarkastaminen on usein tarpeellista, jos tässä vaiheessa ongelmaan ei ole löytynyt ratkaisua.

Kuvassa 8 nähdään esimerkki hallintajärjestelmän päivitykseen liittyvästä lokitiedostosta.



Kuva 8. Vianmääritys lokitiedostoista Windows Server-palvelimella.

5 Tulokset

5.1 Havainnot

Hallintajärjestelmän käyttöönotto ei ole helppoa ilman riittäviä resursseja. Kun hallintajärjestelmää otetaan käyttöön, on hyvä varata riittävästi keskusmuistia sen toimintaa varten. Suositukseni on vähintään 32 GB keskusmuistia sen sujuvan toimivuuden kannalta. Testiympäristössä oli asennettuna 24 GB keskusmuistia, joka aiheutti ongelmia suorituskyvyssä.

Järjestelmä ei ole tehokas, jos agenttia ei asenneta kokonaisvaltaisesti organisaation päätelaitteille. Tehokkuutta vähentää, jos osalla laitteista on agentti asennettuna ja osalla ei.

Käyttöjärjestelmät, joille agentti on asennettu ja jotka ovat vanhoja, eivät välttämättä tule hallintajärjestelmään näkyviin. Testiympäristössä agentti toimi parhaiten Windows Server 2016 ja Windows Server 2019 -käyttöjärjestelmillä.

Yksi havainnoista on, että hallintajärjestelmän käyttäminen voi vaatia IT-tiimin koulutusta. Sen käyttämiseen on hyvä järjestää koulutusta organisaatiossa, jotta sen käyttäminen olisi tehokasta ja sujuvaa.

5.2 Käyttöönoton riskit

Vaikka hallintajärjestelmän tehtävä on pienentää organisaation hyökkäysrajapintaan kohdistuvia riskejä, kuuluu sen käyttöönottoprosessiin myös riskejä kuten kaikissa IT-järjestelmissä.

Yleisiä riskejä, joita havainnointiin hallintajärjestelmän käyttöönotossa kohdistuvat pääasiassa siihen, kuinka ylläpitäjä määrittää hallintajärjestelmän. Jos hallintajärjestelmä määritetään vääränlaisilla asetuksilla, voi se aiheuttaa ongelmia kuten altistaa sille, että päätelaitteiden määritys hallintajärjestelmään jää puutteelliseksi tai päätelaitteita jää kokonaan lisäämättä järjestelmään.

Käyttöönottoon liittyvissä riskeissä korostuu myös hallintajärjestelmän resurssien käyttäminen. Esimerkiksi hallintajärjestelmän moottoria ei tulisi asentaa palvelimelle, jota käytetään myös muuhun tarkoitukseen koska moottori

käyttää paljon keskusmuistia, eikä moottoria saa altistaa muiden ohjelmien aiheuttamille uhkille. Jos moottorilla ei ole riittäviä resursseja toimiakseen, voi se aiheuttaa ongelmia koko järjestelmän käytössä eikä lopputuloksena ole kokonaisvaltaisesti hallittu haavoittuvuuksien hallintajärjestelmä. Jos samalla palvelimella on asennettuna muita ohjelmia, voi hallintajärjestelmän palvelimesta, jossa moottori on asennettuna tulla haavoittuva.

5.3 Käyttöönoton haasteet

Haasteet käyttöönotossa osoittautuvat pääasiassa fyysisten resurssien riittävyyteen. Hallintajärjestelmän moottorin asennuksen seurauksena keskusmuistin määrä väheni liikaa, jonka korjaamiseksi piti lisätä keskusmuistia palvelimelle.

Palomuurisäännöt on oltava riittävät verkoissa. Palvelimen on pystyttävä keskustelemaan internetin kautta Rapid7-pilvihallinnan kanssa, jotta paikallinen moottori löytää päätelaitteen. Mikäli päätelaite on eristetyssä verkossa, josta on rajallinen pääsy internetiin, on tärkeää varmistaa, että verkosta on sallittu liikenne tarvittaviin verkko-osoitteisiin. Opinnäytetyön testiympäristössä palomuurilla oli segmentoitu päätelaitteiden verkot erilleen, joten palomuurisäännöt määritettiin palomuurilaitteeseen, jotta keskustelu pilvihallinnan kanssa onnistui.

Haasteita oli vanhempien käyttöjärjestelmien kanssa. Kun agentti asennettiin vanhemmalle päätelaitteelle kuten Windows Server 2012, se ei tullut näkyviin hallintajärjestelmään. Hallintajärjestelmän käyttöönotossa on suunniteltava tarkkaan, että organisaation päätelaitteet ovat riittävän uusia ja että hallintajärjestelmä tukee käyttöjärjestelmää.

5.4 Johtopäätökset ja suositukset

Opinnäytetyössä käyttöönotettu hallintajärjestelmä on toimiva ratkaisu organisaation tietojärjestelmien kyberturvallisuuden haavoittuvuuksien hallintaan. Käyttöönoton jälkeen IT-tiimillä on paljon selkeämpi näkyvyys päätelaitteisiin. Yksi johtopäätöksistä on, että tietoturva ja kyberturvallisuus eivät voi olla hallittuja ilman vastaavaa järjestelmää. Ilman vastaavanlaista

järjestelmää, haavoittuvuudet jäävät pimentoon. Jos haavoittuvuudet jäävät pimentoon, voi tietoturvaan syntyä ongelmia.

5.5 Testitulokset ja analyysit

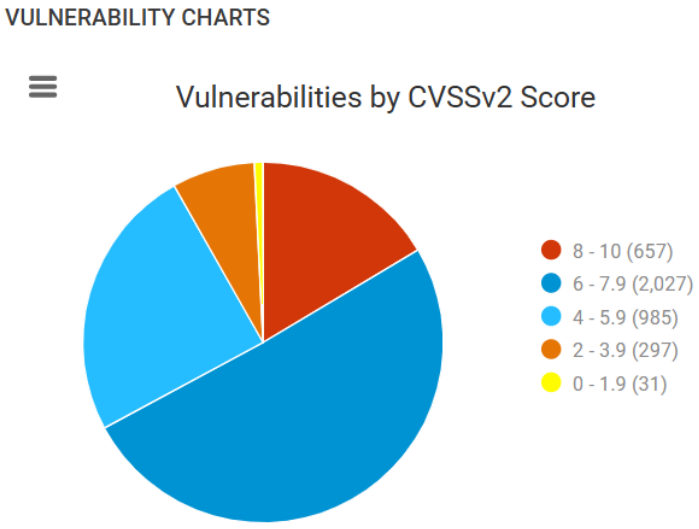
Hallintajärjestelmän avulla on mahdollista tuottaa valmiita raportteja päätelaitteiden tilasta. Raportointimuotoja on monenlaisia.

Kun hallintajärjestelmään kirjaudutaan sisään, nähdään päänäkymässä yleiskuva päätelaitteiden tilasta. Kuvassa 9 nähdään, että päätelaitteita on 4 ja päätelaiteella ”192.168.40.2 ” on korkein riskiarvio.

Kuva 9. Rapid7-hallintajärjestelmän yleiskuva päätelaitteista.

Kun hallintajärjestelmässä siirrytään haavoittuvuuksienhallinnan välilehdelle, nähdään kokonaiskuva kaikkien päätelaitteiden haavoittuvuuksista. Kuvasta 10 voidaan päätellä, että testiympäristössä on päätelaitteita, joilla on kriittisiä

haavoittuvuuksia. Kuvaaja päivittyy automaattisesti skannauksien yhteydessä.



Kuva 10. Rapid7-hallintajärjestelmän yleiskuva päätelaitteiden haavoittuvuuksien riskipitoisuudesta.

Hallintajärjestelmä kertoo listassa suoraan kokonaiskuvan haavoittuvuuksista luokitellen ne järjestykseen haavoittuvuuden pisteytyksen ja kriittisyyden mukaan (Kuva 11).

Title	CVSSv2	CVSSv3	Risk	Published On	Modified On	Severity	Instances
Microsoft Windows: CVE-2023-36874: Windows Error Reporting Service Elevation of Privilege Vulnerability	6.8	7.8	1,000	Mon Jul 10 2023	Thu Sep 05 2024	Severe	3
Microsoft Windows: CVE-2023-36884: Windows Search Remote Code Execution Vulnerability	7.6	7.5	1,000	Mon Jul 10 2023	Thu Sep 05 2024	Critical	3
Microsoft Windows: CVE-2019-0541: MSHTML Engine Remote Code Execution Vulnerability	9.3	8.8	1,000	Mon Jan 07 2019	Tue Aug 06 2024	Critical	2
Microsoft Windows: CVE-2019-0543: Microsoft Windows Elevation of Privilege Vulnerability	4.6	7.8	1,000	Mon Jan 07 2019	Tue Sep 10 2024	Severe	2
Microsoft Windows: CVE-2019-0863: Windows Error Reporting Elevation of Privilege Vulnerability	7.2	7.8	1,000	Mon May 13 2019	Tue Sep 10 2024	Severe	2
Microsoft Windows: CVE-2019-0752: Scripting Engine Memory Corruption Vulnerability	7.6	7.5	1,000	Mon Apr 08 2019	Thu Sep 05 2024	Critical	2
Microsoft Windows: CVE-2019-0803: Win32k Elevation of Privilege Vulnerability	7.2	7.8	1,000	Mon Apr 08 2019	Tue Sep 10 2024	Severe	2
Microsoft Windows: CVE-2019-1388: Windows Certificate Dialog Elevation of Privilege Vulnerability	7.2	7.8	1,000	Mon Nov 11 2019	Tue Sep 10 2024	Severe	2
Microsoft Windows: CVE-2019-1215: Windows Elevation of Privilege Vulnerability	7.2	7.8	1,000	Mon Sep 09 2019	Tue Sep 10 2024	Severe	2
Microsoft Windows: CVE-2021-1675: Windows Print Spooler Remote Code Execution Vulnerability	9.3	7.8	1,000	Mon Jun 07 2021	Mon Sep 23 2024	Critical	3

Kuva 11. Lista löydetyistä haavoittuvuuksista päätelaitteella.

Testitulokset osoittavat, että hallintajärjestelmä automaattisesti tunnistaa, kun haavoittuvuus on korjattu tai päätelaite on kovennettu. Esimerkiksi kun opinnäytetyön pentestaus osiossa hyödynnettiin haavoittuvuutta palvelimelle tunkeutumiseen, jonka jälkeen palvelin päivitettiin. Haavoittuvuus oli päivityksen jälkeen poistunut listalta. Kun haavoittuvuus on poistunut listalta, on haavoittuvuus korjattu päätelaitteella.

6 Yhteenveto

Opinnäytetyön tavoite oli rakentaa kokonaisvaltainen haavoittuvuuksien hallintajärjestelmä konesaliympäristön kaltaiselle alustalle. Opinnäytetyössä asennettiin testiympäristö asennusohjeen mukaisesti ja otettiin käyttöön Rapid7 Insightvm -hallintajärjestelmä toimimaan päätelaitteiden pääkeskuksena.

Asennuksen yhteydessä käytiin myös läpi asennus päätelaitteille, jotka tässä tapauksessa ovat palvelimia. Työssä käsiteltiin haavoittuvuuksien hallintaa viitaten laadittuun ohjeistukseen.

Validointitestien tulosten perusteella työ osoitti haavoittuvuuksien hallintajärjestelmän tärkeyden. Tämä vahvistaa, että haavoittuvuuksien hallintajärjestelmä on välttämätön konesaliympäristöissä, joissa palvelimia on erityisen paljon. Hallintajärjestelmä on myös yksi NIS2-direktiivin edellytyksistä, joka koskee pääasiassa kaikkia IT-palveluntarjoajia.

Työssä käytettiin apuna hallintajärjestelmän tuottamia raportteja löydetyistä haavoittuvuuksista, joita on käsitelty asennusoppaassa. Löydettyjä haavoittuvuuksia käytettiin validointivaiheissa testaukseen.

Lähteet

Blackduck 2025. Penetration Testing. Viitattu 30.4.2025. https://www.blackduck.com/glossary/what-is-penetration-testing.html.

Broad J. & Bindner A. 2013. Hacking with Kali: practical penetration testing techniques. Elsevier Science & Technology books.

Elisa 2021. Zero Trust – Nollaluottamus modernin turvallisen ICT-ympäristön perustana. Blogi 21.3.2021. Viitattu 30.4.2025. https://yrityksille.elisa.fi/ideat/zero-trust-nollaluottamus-turvaa-ict-ymparistosi/.

Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta. EUVL L 333, 27.12.2022, s. 80—152. ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

Garn D. 2025. Top 21 Kali Linux tools and how to use them. Informa TechTarget. Viitattu 29.4.2025. https://www.techtarget.com/searchsecurity/tip/Top-Kali-Linux-tools-and-how-to-use-them#:~:text=Kali%20Linux%20is%20the%20OS,almost%20every%20aspect%20of%20cybersecurity.

Gartner 2025. Vulnerability assessment reviews and ratings. Viitattu 29.4.2025. https://www.gartner.com/reviews/market/vulnerability-assessment.

ISO 2022. ISO/IEC 27001. 2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Viitattu 29.4.2025. https://www.iso.org/standard/27001.

ISO/IEC 27000 Tietoturvallisuuden standardisarja. 2023. Julkaisu SFS Suomen Standardit Ry:n verkkosivuilla. 28.3.2023. Viitattu 10.5.2025. https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/.

Kali Linux. 2025. The most advanced Penetration Testing Distribution. Viitattu 10.5.2025. https://www.kali.org/get-kali/#kali-platforms.

Laulainen O. 2024, Haavoittuvuuden hallinnan teknisen tilanneymmärryksen muodostaminen. Opinnäytetyö (YMK). Teknologialiiketoiminnan johtaminen. Jyväskylä: Jyväskylän ammattikorkeakoulu. https://urn.fi/URN:NBN:fi:amk-2024052314762.

Rapid 7. 2025a. What is InsightVM? Viitattu 30.4.2025. https://docs.rapid7.com/insightvm/.

Rapid 7. 2025b. Troubleshooting. Viitattu 30.4.2025. https://docs.rapid7.com/nexpose/troubleshooting/.

Roytman M. & Bellis E. 2023. Modern vulnerability management: predictive cybersecurity. 1st edition. Artech House.

Ruottinen J. 2023. Haavoittuvuuksien hallintaprosessi ja -järjestelmä kohdeyrityksessä. Opinnäytetyö (ylempi AMK). Kyberturvallisuuden koulutus. Kaakkois-Suomen ammattikorkeakoulu. https://urn.fi/URN:NBN:fi:amk-2023051711402.

SFS-EN ISO 27001. 2023. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS ry. Saatavilla https://sales.sfs.fi/fi/index.html.stx.

Tepa-termipankki 2023. Erikoisalojen sanastojen ja sanakirjojen kokoelma. Sanastokeskus. Viitattu 30.4.2025. https://termipankki.fi/tepa/fi/haku/haavoittuvuus.

Traficom 2020. Haavoittuvuudet - miten niistä ilmoitetaan oikein. Viitattu 29.4.2025. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-miten-niista-ilmoitetaan-oikein.

Traficom 2022. Kyberturvallisuuden vahvistaminen suomalaisissa organisaatioissa. Ohje johdolle ja asiantuntijoille. Viitattu 29.4.2025. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Kyberturvallisuuden_vahvistaminen_suomalaisissa_organisaatiossa_-_ohje_johdolle_ja_asiantuntijoille.pdf

Traficom 2024. Erittäin kriittiset toimialat ja muut kriittiset toimialat. Viitattu 29.4.2025. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM_NIS2_taulukko_230424.pdf.

Virkkula J. 2023. Opas penetraatiotestaukseen. Opinnäytetyö (AMK). Tieto- ja viestintätekniikka. Hämeen ammattikorkeakoulu. https://urn.fi/URN:NBN:fi:amk-2023052212495.

VPN Unlimited 2025a. Haavoittuvuuksien hallinta. Penetraatiotestaus. Viitattu 23.4.2025. https://www.vpnunlimited.com/fi/help/cybersecurity/vulnerability-management?srsltid=AfmBOooQ2Fq1c1pyt9allEOevsWLNQC8u7W4p4P8rtxZj7oRLPO7hK_c.

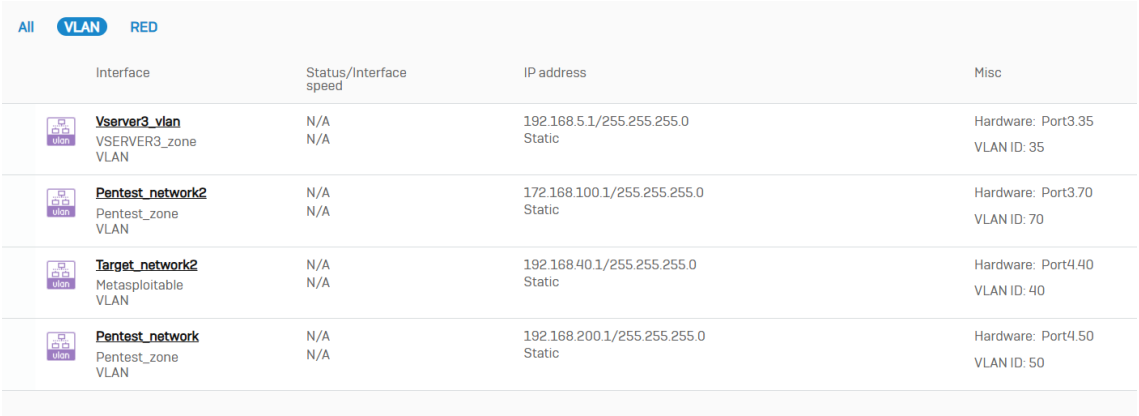
VPN Unlimited 2025b. Haavoittuvuuksien hallinta. Korjaaminen. Viitattu 10.5.2025. https://www.vpnunlimited.com/fi/help/cybersecurity/vulnerability-management?srsltid=AfmBOooi4WU-OOOUlan0mbT9zaDSBt0Gew7_SHHS7lBvBf8Vt3XkxYrj

Yli-Hietanen K. 2021. ISO/IEC 27001 -standardin sertifiointiin valmistautuminen IT-alan yrityksessä. Opinnäytetyö (AMK). Tuotantotalouden tutkinto-ohjelma. Satakunnan ammattikorkeakoulu. https://urn.fi/URN:NBN:fi:amk-202105077576.

Hallintajärjestelmän asennusohje

Tietoverkot

Ennen asennusta on tärkeää määrittää verkkoasetukset palomuuriin ja segmentoida palvelimet omiin verkkoihin käyttämällä virtuaalisia verkkoja (VLAN). Verkkojen eriyttäminen mahdollistaa turvallisen ja hallitun testiympäristön perustamisen. Kuvassa 1 nähdään palomuurissa luodut virtuaaliset verkot virtuaalipalvelimia varten.



Kuva 1. Verkkojen hallinta palomuurissa.

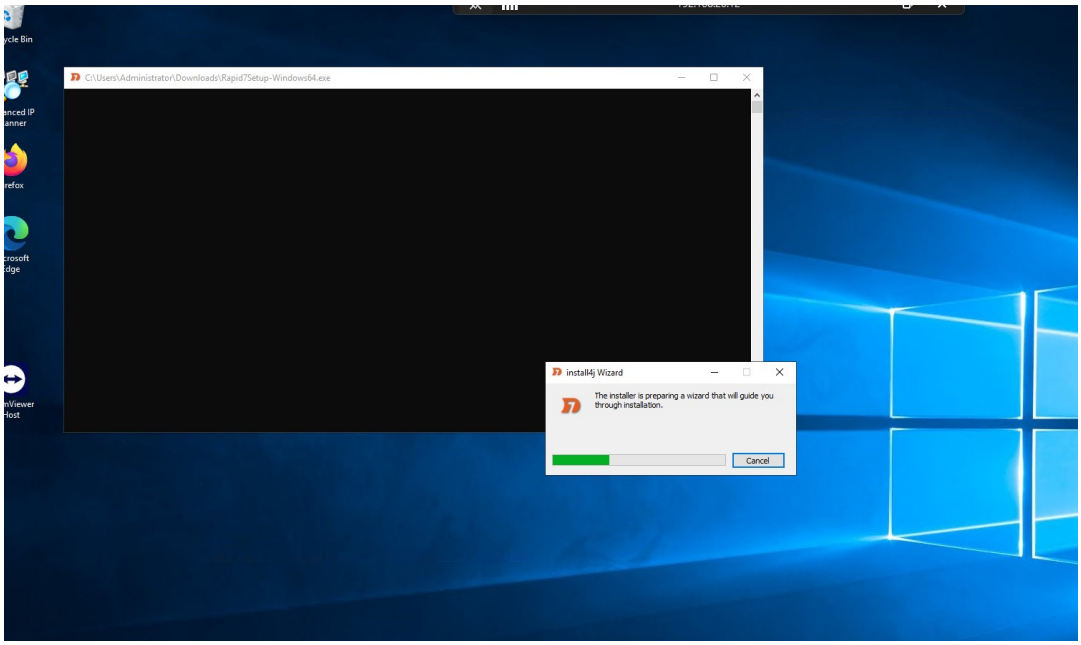
Isäntäpalvelimille voidaan asentaa virtuaalipalvelimia, joita käytetään kohdepalvelimina. Virtuaalipalvelimille voidaan asettaa käytettäväksi oma virtuaaliverkko, joka on mahdollista määrittää Hyper-V-virtualisoinnin asetuksissa isäntäpalvelimilla.

Tässä opinnäytetyössä otetaan käyttöön Rapid7-haavoittuvuuksien hallintajärjestelmä testiympäristössä. Rapid7 Insightvm on saatavilla Rapid7 virallisilta nettisivuilta.

Asentaminen palvelimelle

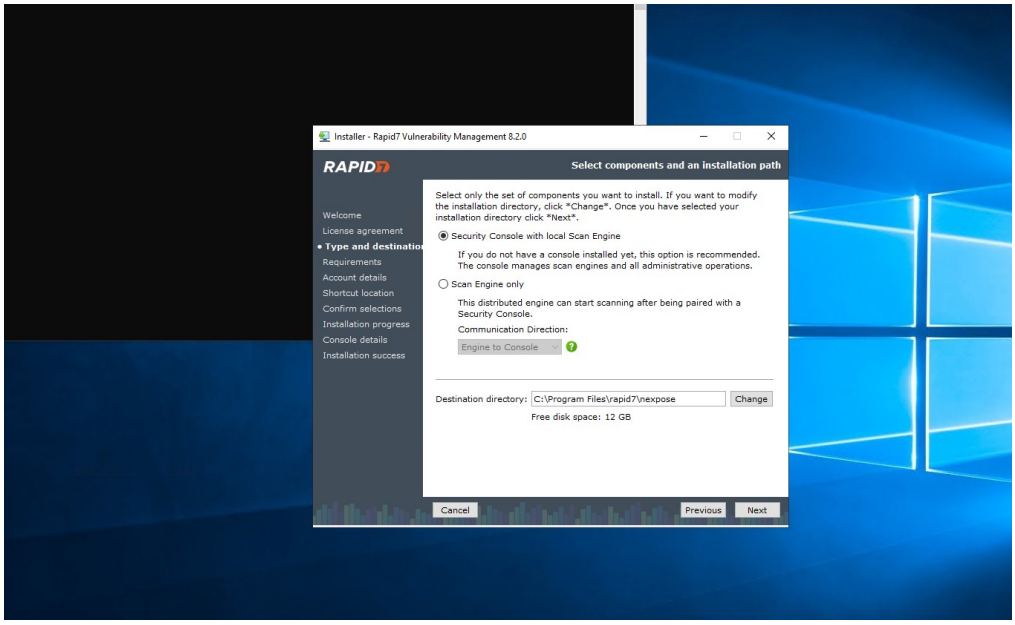
Ohjelmiston mukana tulee asennuspaketti esimerkiksi Windows ja Linux käyttöjärjestelmille (Kuva 2). Tässä tapauksessa Rapid7 asennetaan Windows Server 2019 -käyttöjärjestelmälle toimimaan hakumoottorina. Asennuspaketissa

tulee asennusohjelma, joka asentaa hallintakeskuksen palveluna palvelimelle ja siihen tarvittavan tietokannan.



Kuva 2. Hallintajärjestelmän asentaminen palvelimelle.

Kun asennusohjelma on käynnistetty, asentajaa pyydetään valitsemaan mitkä ominaisuudet asennetaan palvelimelle ja mitkä ominaisuuksista otetaan käyttöön. Opinnäytetyössä käytetään kaikkia mahdollisia ominaisuuksia, joten asennuksessa valittiin ”Security console with local scan engine” (Kuva 3).



Kuva 3. Hallintajärjestelmän asennusohjelma.

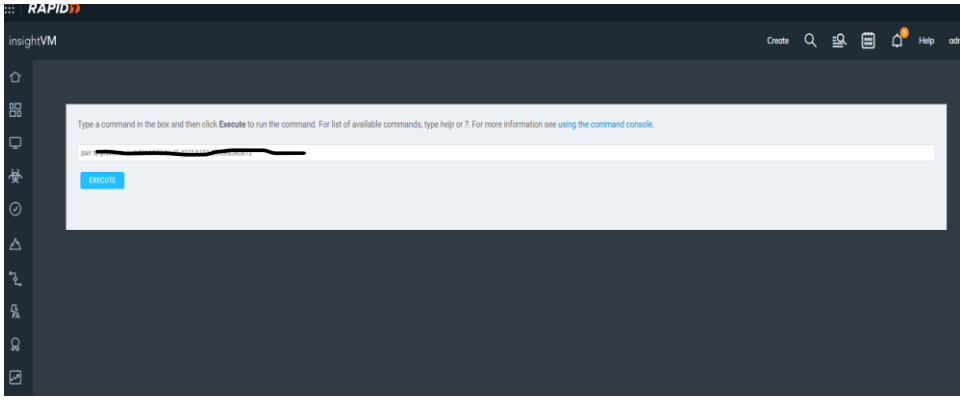
Asennusohjelman valmistuttua, järjestelmän hallintakeskus on valmiina käytettäväksi. Hallintakeskus voidaan nyt avata paikallisesti. Tässä tapauksessa palvelimen paikallinen ip-osoite on 192.168.20.12 ja Rapid7 vakioportti on 3780. Hallintakeskus voidaan siis avata paikallisesti osoitteessa https://192.168.20.12:3780/login.jsp.

Kun hallintakeskus aukeaa esimmäisen kerran, tulee Rapid7 aktivoida lisenssikoodilla. Tämän jälkeen Rapid7 yhdistetään pilvihallintaan. Pilvihallinnan sivuilla on mahdollista luoda käyttäjä ja liittymiskoodi. Liittymiskoodilla voidaan yhdistää paikallinen hallintakeskus pilvihallintaan. Tämä mahdollistaa paikallisen hallintakeskuksen ja pilvihallinnan keskustelun keskenään.

Liittäminen pilvihallintaan

Keskustelu paikallisen hallintakeskuksen ja pilvihallinnan välille kannattaa tehdä mahdollisimman pian sen jälkeen, kun paikallinen hallintakeskus on asennettu. Toimenpidettä varten on ensin kirjauduttava pilvihallintaan ja valittava yhdistä hallintakeskus (engine). Tämä luo valmiin komennon satunnaisella numerosarjalla. Komento kopioidaan ja liitetään paikallisen hallintakeskuksen komentoriville kuvan 4 mukaisesti.

Liitoksen jälkeen paikallinen hallintajärjestelmä välittää tietoja pilvihallintaan ja järjestelmän hallinta on suurimmaksi osaksi mahdollista pilvihallinnan kautta. Tämä on turvallisempaa koska pilvihallinnan käyttämisessä on mahdollista käyttää kaksivaiheista todennusta, eikä paikallista palvelua tarvitse avata internetistä käytettäväksi, joka nostattaisi väärinkäytön mahdollisuutta.



Kuva 4. Liittäminen pilvihallintaan.

Pääsynhallinta

Hallintajärjestelmässä on aluksi vain yksi hallintakäyttäjä, jolla kirjautuminen paikallisesti on mahdollista. Seuraavaksi voidaan konfiguroida fyysiseen palomuuriin VPN-yhteys, jonka avulla hallintakeskusta voidaan käyttää muualta kuin palvelimelta.

Päätelaitteiden lisääminen hallintakeskukseen

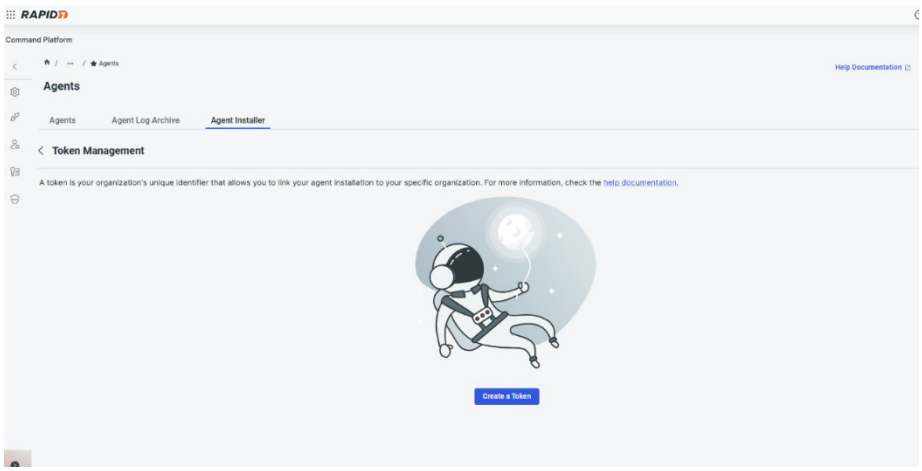
Rapid7-hallintajärjestelmässä päätelaitteiden hallinta on selkeää ja melko yksinkertaista. Tässä opinnäytetyössä otettiin käyttöön Rapid7-hallintajärjestelmä konesalia jäljittelevään ympäristöön, joten päätelaitteiden hallinta suunniteltiin siihen sopivaksi.

Hallintajärjestelmä yhdistetään pilvihallintaan, jolloin hallintajärjestelmää voidaan tarkastella pilvihallinnan kautta. Pilvihallinta on Rapid7:n omilla palvelimilla toimiva hallintajärjestelmä, joka mahdollistaa paikallisen hallintajärjestelmän käyttämisen internetin kautta suojatusti sen sijaan että

paikalliseen hallintajärjestelmään avattaisiin pääsy palomuurin NAT-säännöillä, joka altistaa palvelimeen kohdistuvien hyökkäyksien riskin.

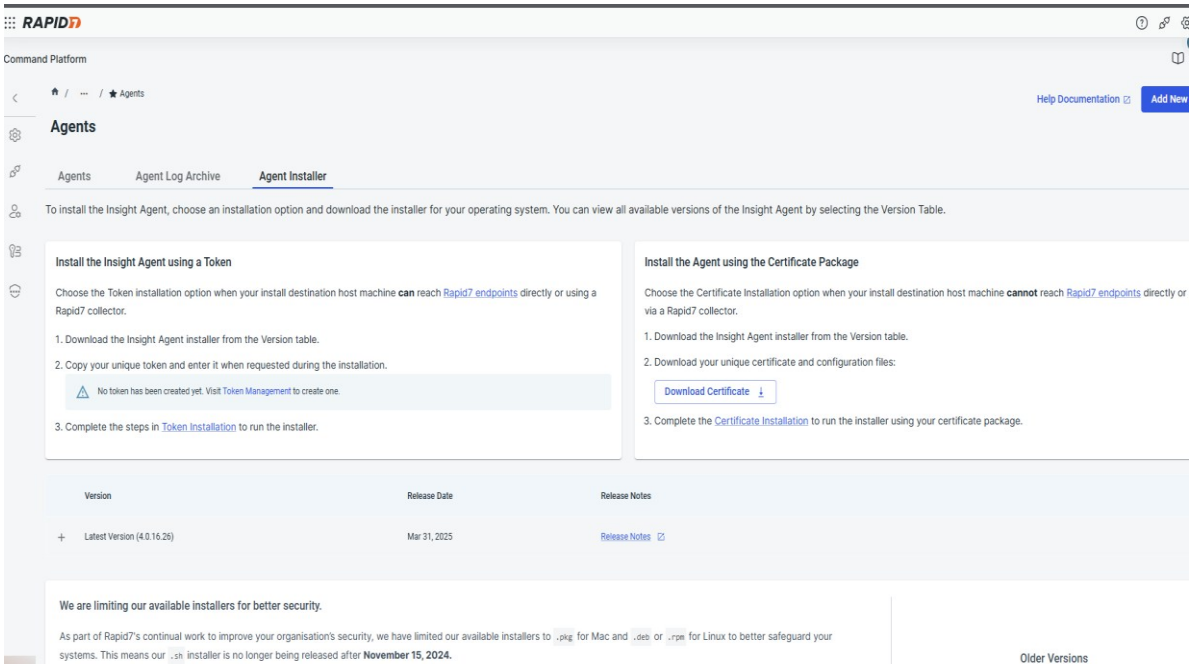
Kun pilviliitos on tehty valmiiksi, käyttäjälle aukeaa hallintapaneeli, josta voidaan luoda asennusohjelmia päätelaitteille. Tätä varten hallintapaneelissa luodaan organisaatiokohtainen numerosarja. Tämän jälkeen hallintapaneelista on asennettavissa käyttöjärjestelmäkohtainen asennuspaketti.

Päätelaitteiden lisäämiseksi on luotava ”agentti” pilvihallintajärjestelmässä (Kuva 5). Tätä varten pilvihallinnassa on ensin luotava satunnainen numerosarja ”token”, jonka avulla päätelaitteeseen asennettu ohjelma muodostaa yhteyden hallintajärjestelmään. Tämän jälkeen luodaan numerosarja ”create token” toiminnolla.



Kuva 5. Päätelaitteen asennuspaketin luominen pilvihallintajärjestelmässä.

Tämän jälkeen voidaan luoda agentti asennettavaksi päätelaitteille, joita haluamme seurata (Kuva 6). Pilvihallinnassa luodaan uusi agentti eli ohjelma, joka etsii haavoittuvuuksia päätelaitteelta.



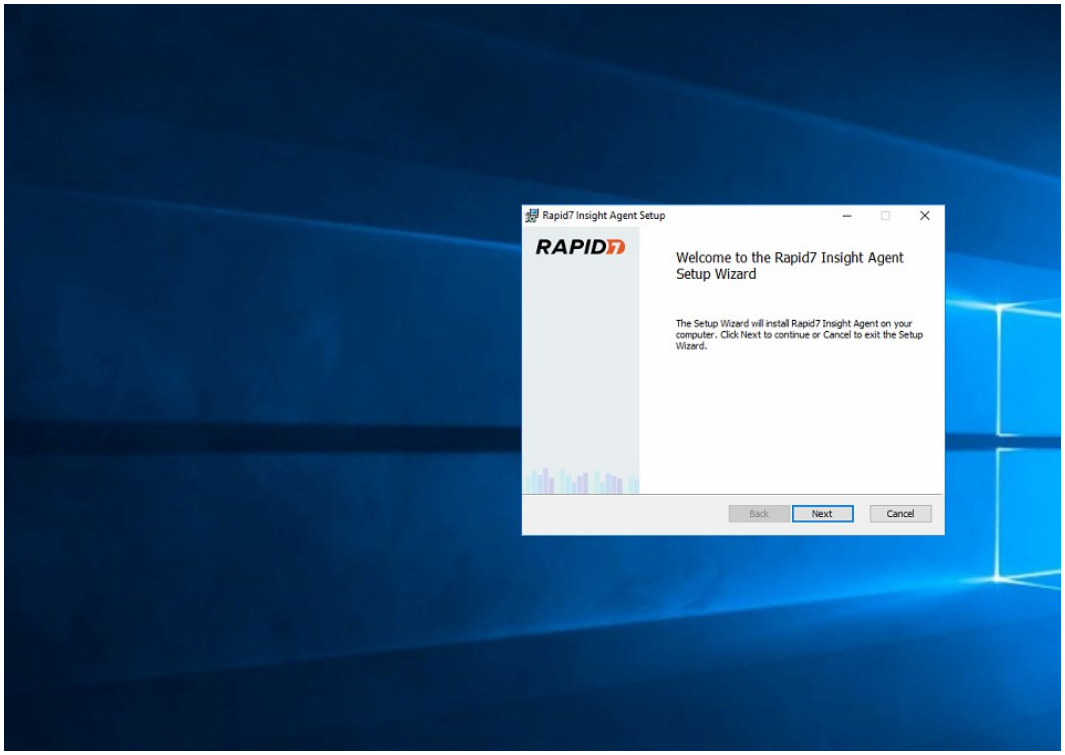
Kuva 6. Päätelaitteen asennuspaketin lataaminen pilvihallintajärjestelmässä.

Asennus päätelaitteille

Pilvihallinnassa luotu agentti voidaan asentaa monelle eri käyttöjärjestelmälle. Tässä tapauksessa käytetään Windows-versiota, koska testiympäristön virtuaalipalvelimet ovat Windows palvelimia.

Asennuksessa käynnistetään asennusohjelma halutulla päätelaitteella ja edetään ohjeiden mukaisesti (Kuva 7). Ohjelma pyytää numerosarjan, joka aikaisemmin on luotu hallintapaneelissa. Numerosarja syötetään asennusohjelmaan. Järjestelmä käyttää numerosarjaa, jotta agentti muodostaa yhteyden oikeaan hallintaympäristöön.

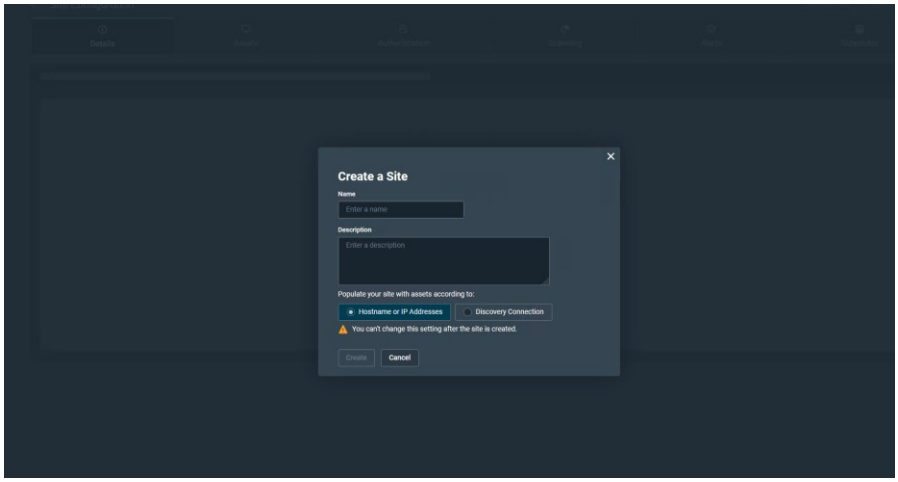
Asennukseen jälkeen agentti on toiminnassa päätelaitteella ja yhdistää paikallisen hallintajärjestelmän kanssa pilvipalvelun liitoksen kautta. Komentokeskus löytää päätelaitteen yleensä muutaman tunnin kuluessa.



Kuva 7. Päätelaitteen agentin asentaminen.

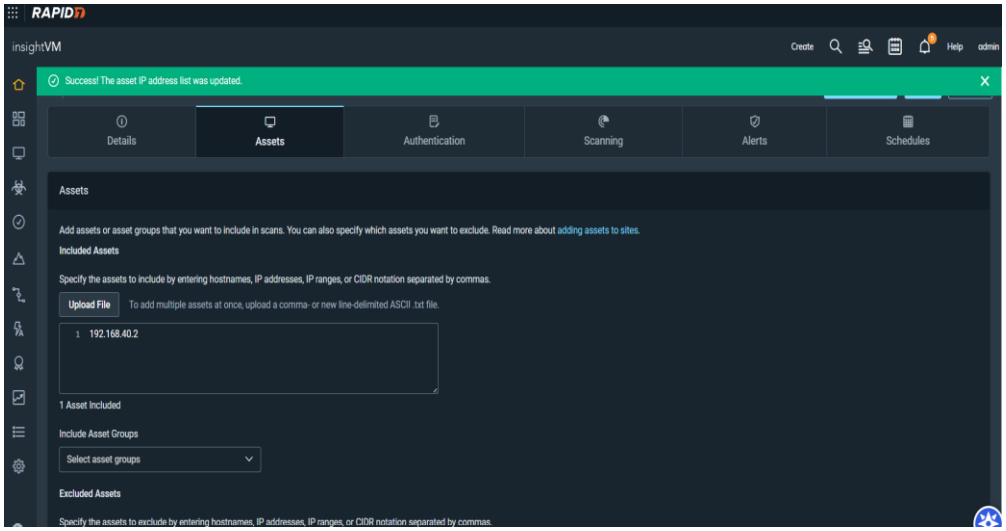
Päätelaitteiden ryhmittely

Päätelaitteiden hallinta kannattaa aloittaa ryhmittelemällä päätelaitteet omiin osastoihin (Kuva 8). Tämä on varsinkin konesaliympäristössä tärkeää, koska se helpottaa päätelaitteiden järjestelyä ja tunnistamista. Konesaliympäristössä voidaan jaotteluun käyttää esimerkiksi asiakasyrityksen nimeä, joka auttaa tunnistamaan päätelaitteen. Luodaan ensimmäinen osasto. Luodaan osasto nimellä opinnäytetyö.



Kuva 8. Päätelaitteiden osastointi.

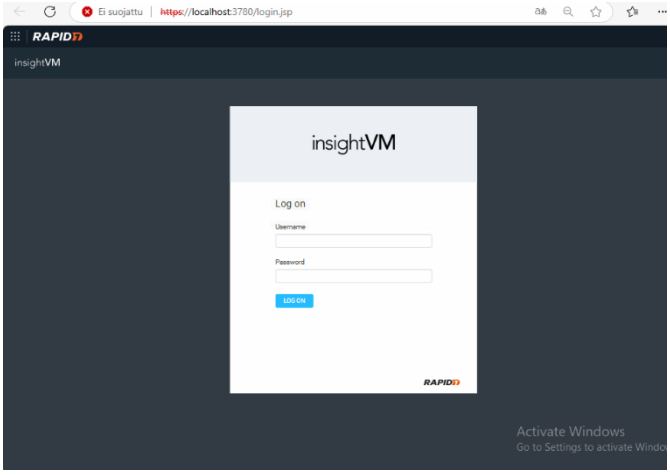
Liitetään seuraavaksi testiympäristön palvelin, jolle agentti on asennettu ja lisätään se osastoon, joka on luotu. Lisääminen onnistuu käyttämällä esimerkiksi IP-osoitetta tai laitteen nimeä (Kuva 9).



Kuva 9. Päätelaitteen lisääminen osastoon.

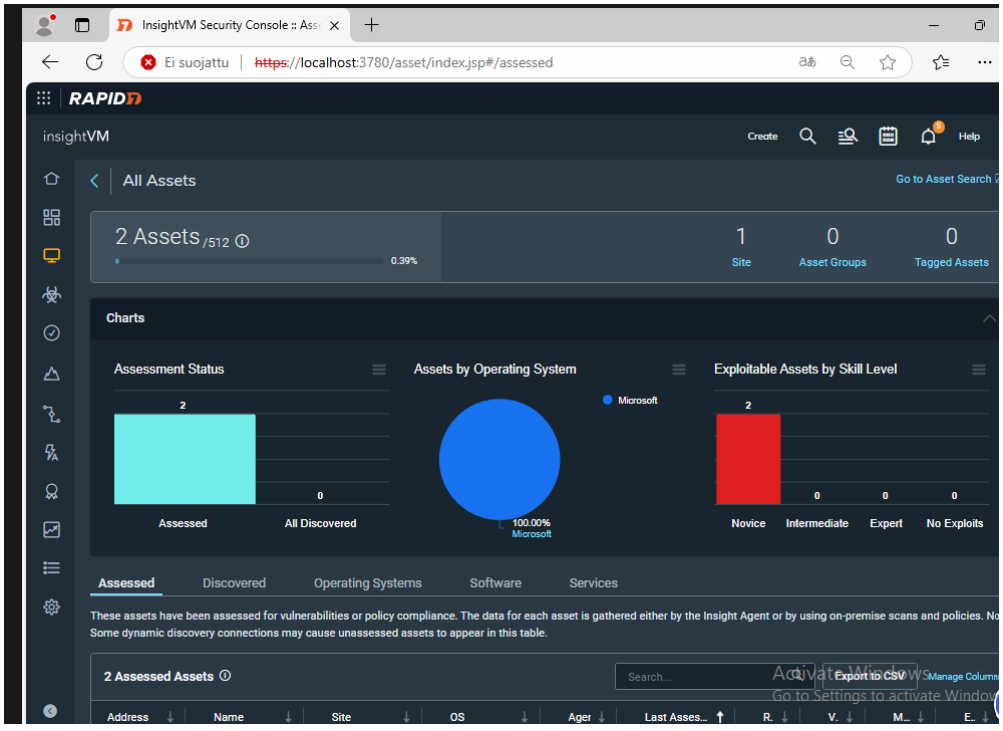
Käyttäminen yleisesti

Hallintasivuston avaaminen pyytää ensin käyttäjätietoja (Kuva 10). Käyttäjätiedot on luotu asennuksen yhteydessä, joita käytetään hallintasivulle kirjautumiseen. Kun sivulle on kirjauduttu sisään aukeaa yleisnäkymä, josta nähdään ympäristön nykytila. Tämä sisältää tietoja uusista haavoittuvuuksista ja laitteiden määrästä.



Kuva 10. Kirjautuminen hallintajärjestelmään.

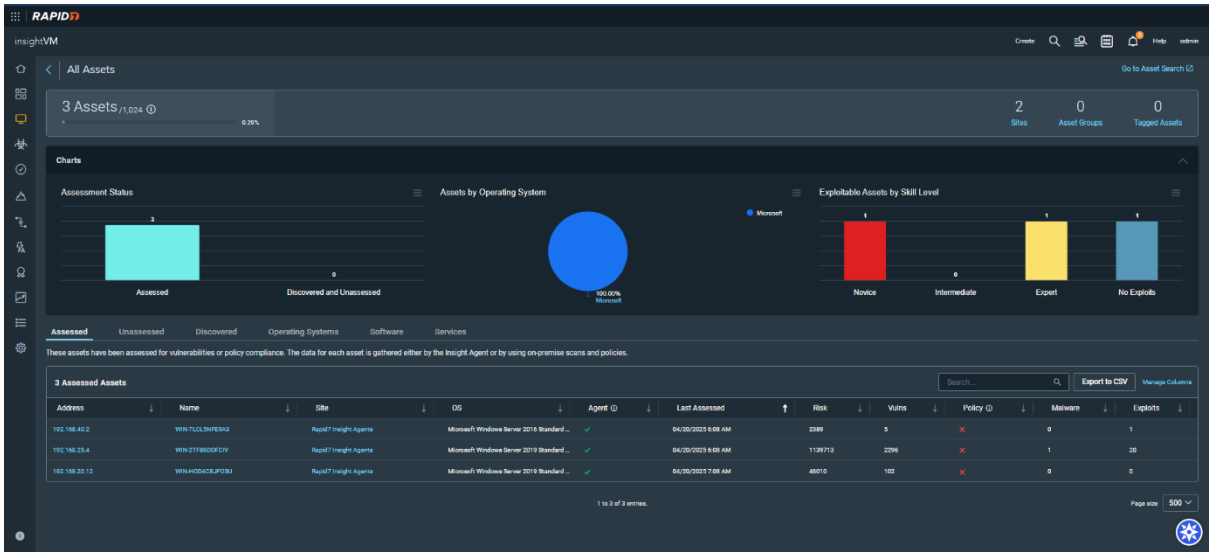
Valikosta aukeaa erilaisia näkymiä. Ensimmäisenä on päätelaitteet. Päätelaitteiden näkymästä voidaan nähdä laitteet, joihin agentti on asennettu (Kuva 11). Päätelaitteita voidaan tarkastella osastoittain.



Kuva 11. Yleisnäkymä päätelaitteista.

Hallintajärjestelmän käyttäminen ja pentestaus

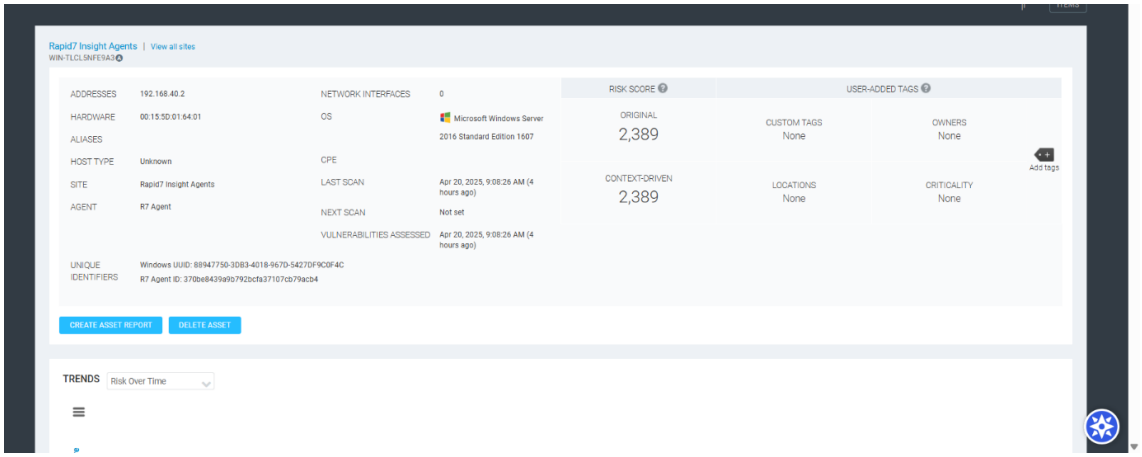
Aloitetaan kirjautumalla paikalliseen hallintapaneeliin. Paikallisessa hallintapaneelissa siirrytään ”Assets” välilehdelle eli päätelaitteiden välilehdelle (Kuva 1).



Kuva 1. Yleisnäkymä päätelaitteista.

Välilehdellä näkyy kolme palvelinta, joille ohjelma on asennettu.

Valitaan valikosta testipalvelin, jota käytämme kokonaissuorituksessa kohteena. Tämän jälkeen aukeaa tarkennettu näkymä, jossa pystytään tarkastelemaan hallintajärjestelmän haavoittuvuuksien tarkistuksien tuloksia päätelaitteilla. Tarkastellaan haavoittuvuuksia ensin raportin kautta. Tehdään raportti päätelaitteesta valitsemalla ”create asset report” (Kuva 2).

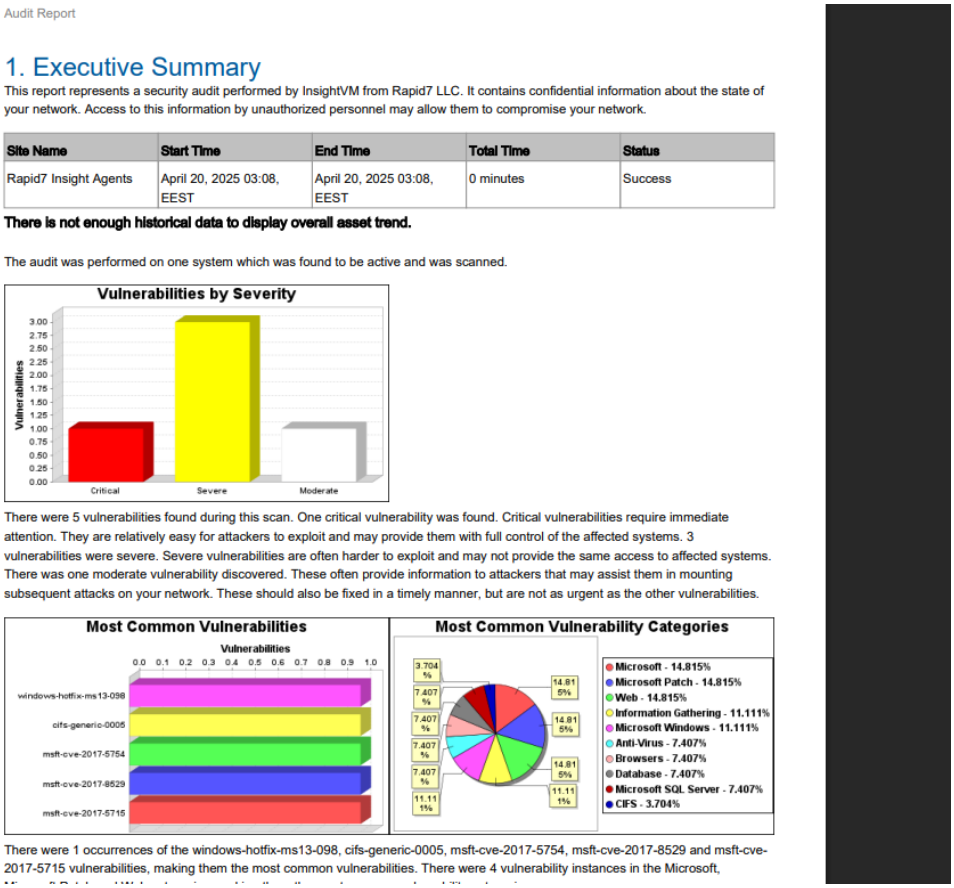


Kuva 2. Raportin luominen hallintajärjestelmässä.

Kuvassa 3 on yleinen raportti Windows Server 2016 -palvelimesta, joka on tässä tapauksessa testipalvelin. Kuvasta 3 nähdään, että palvelimelta on löytynyt haavoittuvuuksia ja osa haavoittuvuuksista ovat kriittisiä tai huomattavia.

Koska palvelimelta on löytynyt huomattavasti haavoittuvuuksia, tulee haavoittuvuudet korjata mahdollisimman nopeasti ja huolellisesti.

Hallintajärjestelmän luoma raportti on ladattavissa pdf-tiedostona. Raporttia voidaan tarkastella tarkemmin, jonka hallintajärjestelmä on luonut.



Audit Report

1. Executive Summary

This report represents a security audit performed by InsightVM from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
Rapid7 Insight Agents	April 20, 2025 03:08, EEST	April 20, 2025 03:08, EEST	0 minutes	Success

There is not enough historical data to display overall asset trend.

The audit was performed on one system which was found to be active and was scanned.

Vulnerabilities by Severity

Vulnerabilities

3.00 2.75 2.50 2.25 2.00 1.75 1.50 1.25 1.00 0.75 0.50 0.25 0.00

Critical Severe Moderate

There were 5 vulnerabilities found during this scan. One critical vulnerability was found. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 3 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There was one moderate vulnerability discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.

Most Common Vulnerabilities

Vulnerabilities

0.0 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1.0

windows-hotfix-ms13-098

cifs-generic-0005

msft-cve-2017-5754

msft-cve-2017-8529

msft-cve-2017-5715

Most Common Vulnerability Categories

3.704 %
7.407 %
7.407 %
7.407 %
7.407 %
11.11 %
14.81 %
14.81 %
14.81 %
11.11 %

Microsoft - 14.815%
Microsoft Patch - 14.815%
Web - 14.815%
Information Gathering - 11.111%
Microsoft Windows - 11.111%
Anti-Virus - 7.407%
Browsers - 7.407%
Database - 7.407%
Microsoft SQL Server - 7.407%
CIFS - 3.704%

There were 1 occurrences of the windows-hotfix-ms13-098, cifs-generic-0005, msft-cve-2017-5754, msft-cve-2017-8529 and msft-cve-2017-5715 vulnerabilities, making them the most common vulnerabilities. There were 4 vulnerability instances in the Microsoft,

Kuva 3. Raportti päätelaitteesta.

Kun raportissa edetään, tulee vastaan tarkennettu lista palvelimelta löydetyistä haavoittuvuuksista. Lista on järjestetty haavoittuvuuden kriittisyyden mukaan. Kuvassa 4 nähdään yksi kriittisistä haavoittuvuuksista, joka on löytynyt palvelimelta. Haavoittuvuuksien alapuolella kerrotaan suoraan mitä toimenpiteitä palvelimella tulee tehdä haavoittuvuuden korjaamiseksi. Tässä tapauksessa korjaus on melko yksinkertaisesti korjattavissa käyttöjärjestelmän päivityksellä.

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. CVE-2013-3900: MS13-098: Vulnerability In Windows Could Allow Remote Code Execution (windows-hotfix-ms13-098)

Description:

This vulnerability could allow remote code execution if a user or application runs or installs a specially crafted, signed portable executable (PE) file on an affected system.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.40.2	Vulnerable OS: Microsoft Windows Server 2016 Standard Edition 1607 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Wintrust\Config - key does not existEnableCertPaddingCheck - value does not exist

References:

Source	Reference
CVE	CVE-2013-3900
URL	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

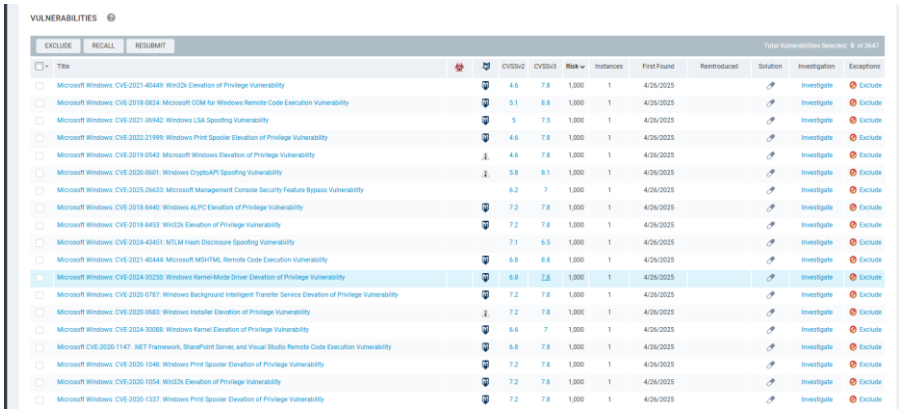
Vulnerability Solution:

Download and apply the patch from: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

Kuva 4. Raportti päätelaitteen haavoittuvuuksista.

Seuraavaksi validoidaan vakava haavoittuvuus testipalvelimella käyttäen pentestaustyökaluja. Haavoittuvuuksia tarkastellaan eettisen hakkerin näkökulmasta eli miten haavoittuvuutta voidaan hyödyntää palvelimelle tunkeutumisessa.

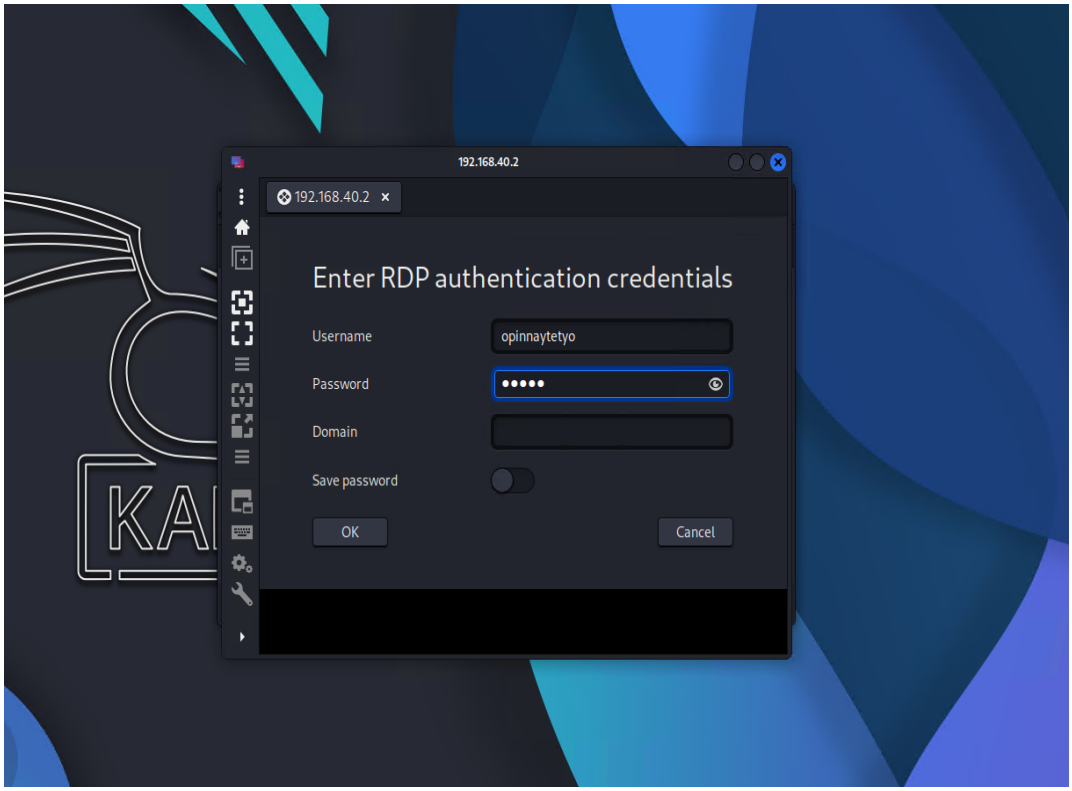
Palvelimen haavoittuvuuksia voidaan tarkastella suoraan haavoittuvuudet-välilehdeltä hallintajärjestelmässä (Kuva 5).



Kuva 5. Lista löydetyistä haavoittuvuuksista.

Skannauksien tulokset on lajiteltu kuvassa 5, sen mukaan mikä on haavoittuvuuden riskiluokka. Haavoittuvuus, joka on ensimmäisenä listalla, on vakava: ”CVE-2021-40449: Win32k Elevation of Privilege Vulnerability”. Käytetään löydettyä haavoittuvuutta validoinnissa.

Voidaan todistaa, että palvelimella on kyseinen haavoittuvuus, jonka avulla ulkopuolinen pystyy saamaan pääkäyttäjän oikeudet palvelimella. Tässä tilanteessa tunkeutujalla on oltava tiedossa tavallinen käyttäjä, jota käyttämällä palvelimelle saa etäyhteyden. Käyttäjän käyttöoikeudet ovat kuitenkin tavalliset, jotka eivät mahdollista ylläpidollisia toimenpiteitä palvelimella. Tämä haavoittuvuus mahdollistaa sen, että tavallisen käyttäjän oikeudet voidaan muuttaa pääkäyttäjän tasoiseksi hyödyntämällä haavoittuvuutta. Palvelimelle voidaan muodostaa etäyhteys käyttäen ”Remmina” nimistä työkalua (Kuva 6).

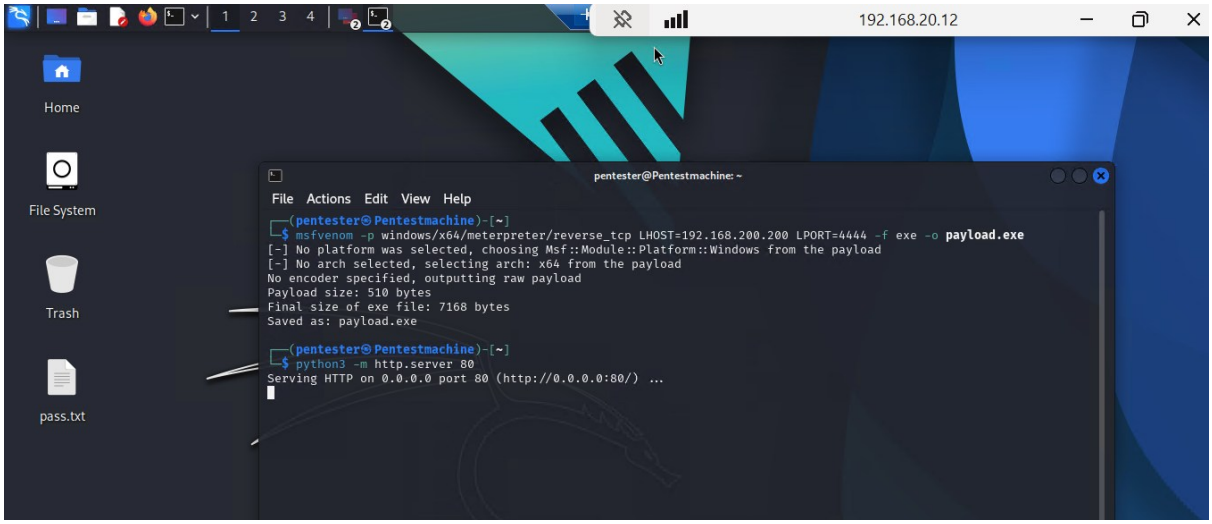


Kuva 6. Etäyhteyden muodostaminen käyttäen Remmina-työkalua.

Tämän haavoittuvuuden hyödyntämiseksi, on tunkeutujalla oltava jonkinlainen pääsy kohteeseen ennestään. Tässä tilanteessa avataan pääsy etätyöpöytäyhteydellä pentestauskoneelta suoraan palvelimelle käyttäen tavallista käyttäjää ilman pääkäyttäjän oikeuksia. Käyttäjän nimi on ”opinnaytetyo”. Etäyhteyden muodostaminen onnistuu ja etätyöpöytä aukeaa (Kuva 7).

Kuva 7. Muodostettu etätyöpöytäyhteys.

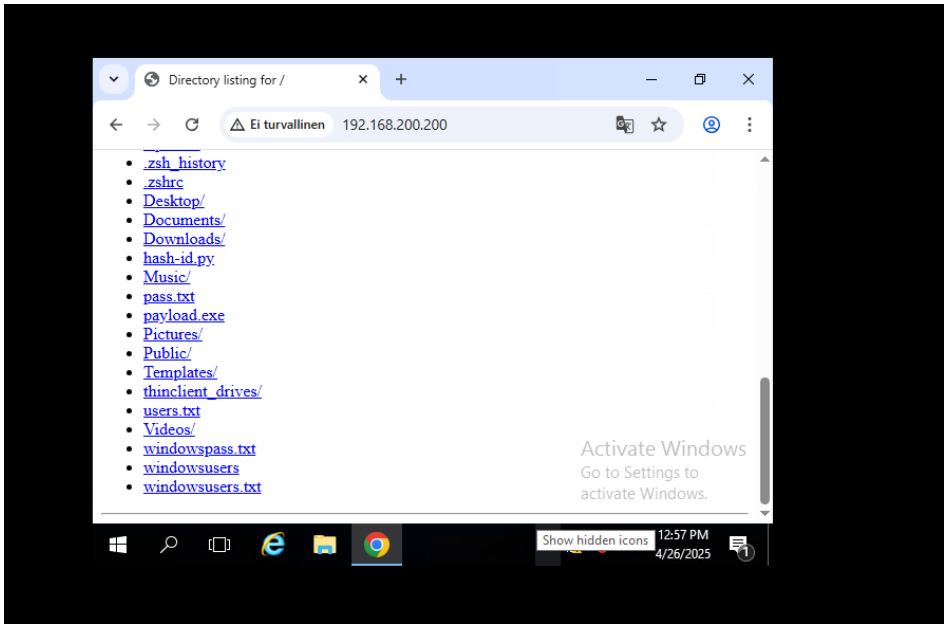
Tämän haavoittuvuuden hyödyntämiseksi tunkeutujan on luotava pentestauskoneella tunkeutumiseen tarvittava ohjelma ja käynnistettävä toimiva paikallinen nettisivupalvelu, jonka kautta kohdepalvelimelle asennetaan tunkeutumiseen tarvittava ohjelma (Kuva 8). Tunkeutumiseen tarvittavaa ohjelmaa kutsutaan ”exploitiksi”. Useilla pentestausohjelmilla on kyky luoda haavoittuvuuden hyväksikäyttöön käytettävä ohjelma. Ensin luodaan ohjelma, joka käynnistää niin kutsutun ”reverseshellin”. Tämä luo automaattisesti ”.exe” päätteisen tiedoston. Seuraavaksi käynnistetään http-sivustopalvelu pentestauskoneella. Sivustoa voidaan käyttää haavoittuvuuden hyväksikäyttöön käytettävän ohjelman siirtämiseen kohdepalvelimelle.



Kuva 8. Paikallisen nettisivupalvelun käynnistäminen.

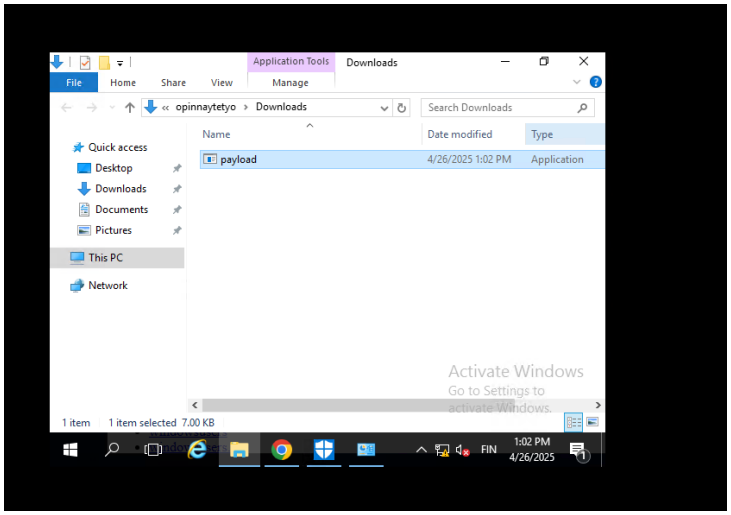
Tämän jälkeen kohdetietokoneelle voidaan siirtyä takaisin aikaisemmin muodostetulla etätyöpöytäyhteydellä. Seuraavaksi voidaan avata sivusto ja ladata ohjelma ”payload.exe”, joka on tässä tapauksessa haavoittuvuuden hyväksikäytön mahdollistava ohjelma (Kuva 9).

Ennen käynnistämistä, käynnistän ”kuuntelijan” pentestauskoneella, joka kuuntelee, kun ohjelma suoritetaan kohdepalvelimella ja muodostaa yhteyden. Tämä mahdollistaa haavoittuvuuden hyväksikäyttöön käytettävän ohjelman hyödyntämisen. Tämän jälkeen ohjelma voidaan ladata palvelimelle sivustolta klikkaamalla ohjelman nimeä (Kuva 9).



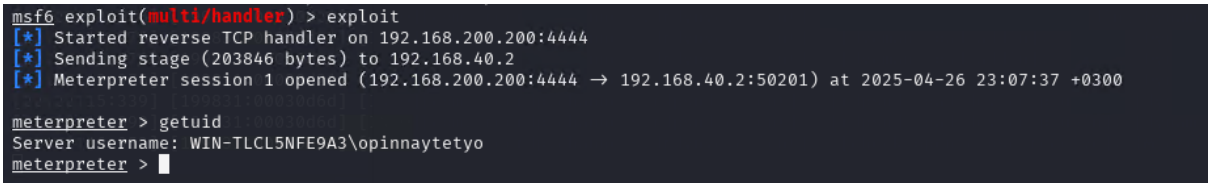
Kuva 9. Haavoittuvuuden hyväksikäytön lataamiseen käytettävä paikallinen verkkosivu.

Ohjelma latautuu ladattujen tiedostojen kansioon resurssienhallinnassa. Tämän jälkeen voidaan käynnistää kuvassa 10 näkyvä haavoittuvuuden hyväksikäytön mahdollistava ohjelma.



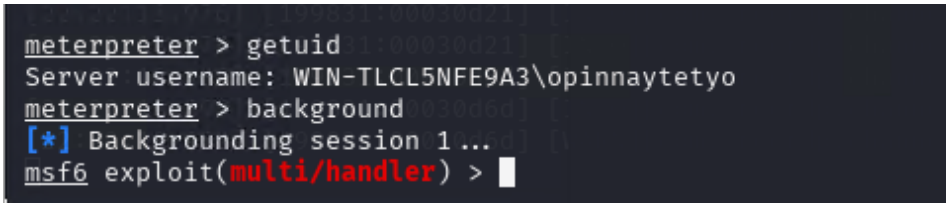
Kuva 10. Haavoittuvuuden hyväksikäytön mahdollistava ohjelma resurssienhallinnassa.

Ohjelman käynnistämisen jälkeen yhteys muodostuu onnistuneesti, jonka jälkeen avautuu meterpreter-yhteys, jota tarvitaan pääkäyttäjän oikeuksien saamiseksi (Kuva 11).



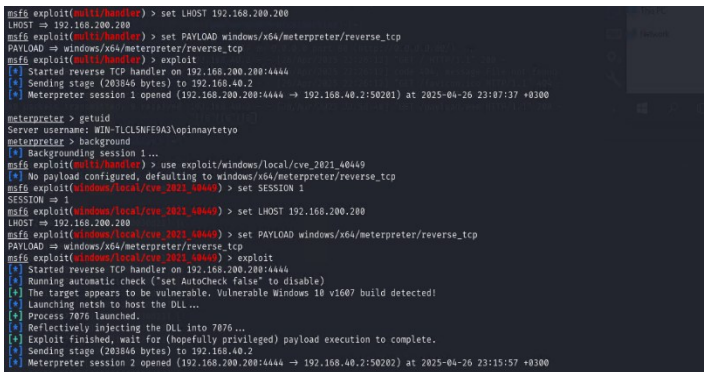
Kuva 11. Muodostettu meterpreter-yhteys tavallisella käyttäjällä.

Varsinainen haavoittuvuus on pääkäyttäjän oikeuksien saaminen hyödyntämällä haavoittuvuutta, joka on löydetty hallintajärjestelmällä. Seuraavaksi voidaan hyödyntää varsinaista haavoittuvuutta pääkäyttäjäoikeuksien saamiseen. Tämä edellyttää kuvassa 12 käytettyä komentoa.



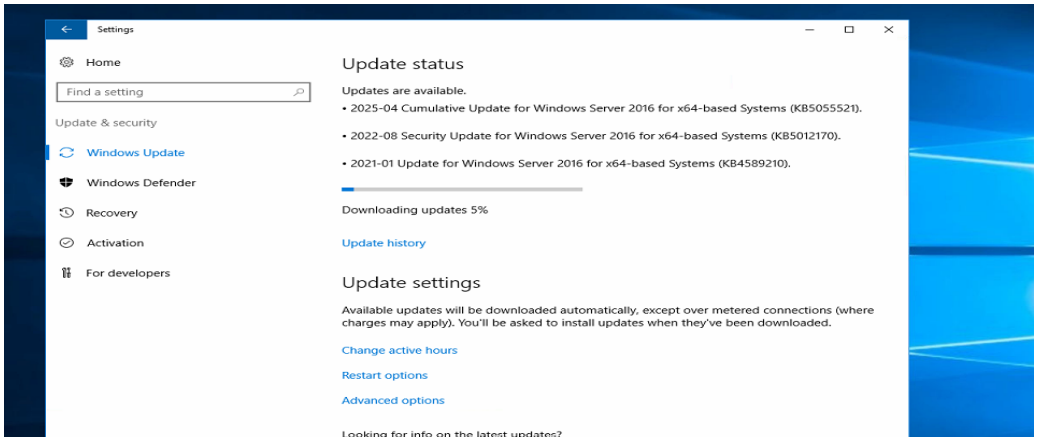
Kuva 12. Background-komennon käyttäminen meterpreter yhteydessä.

Haavoittuvuuden hyödyntämiseksi, voidaan pentestauskoneella käyttää Metasploit-työkalua ja hyödyntää sen toimintoja. Metasploit voidaan ohjata käyttämään haavoittuvuuteen toimivia tunkeutumismenetelmiä, jonka avulla voidaan korottaa pääkäyttäjäoikeudet palvelimelle (Kuva 13).



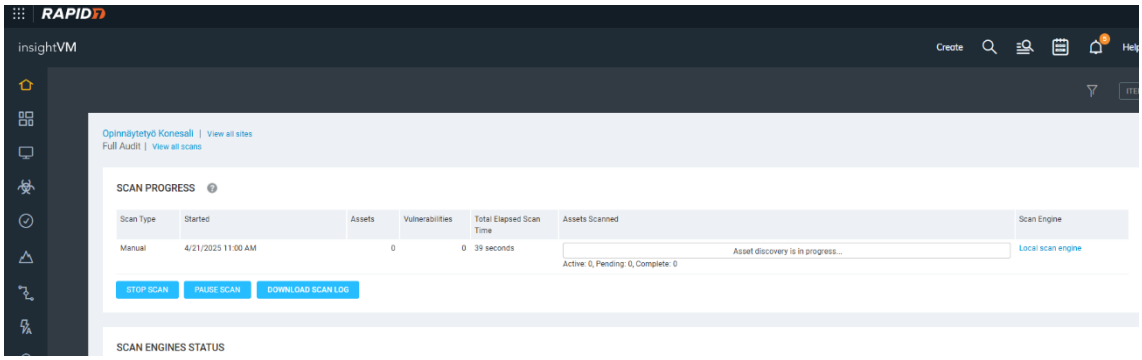
Kuva 13. Pääkäyttäjäoikeuksien korottaminen Metasploit-työkalulla.

Seuraavaksi validoitu haavoittuvuus voidaan korjata. Ensimmäisenä asennetaan puuttuvat päivitykset palvelimelle (Kuva 14).



Kuva 14. Päivityksien asentaminen palvelimelle.

Palvelimen päivityksen jälkeen voidaan suorittaa haavoittuvuuksien tarkistus. Automaattinen haavoittuvuuksien tarkistus voi kestää pidempään, jonka vuoksi on suositeltavaa tehdä tarkistus käsin. Voidaan tehdä manuaalinen haavoittuvuuksien tarkistus hallintapaneelissa (Kuva 15).



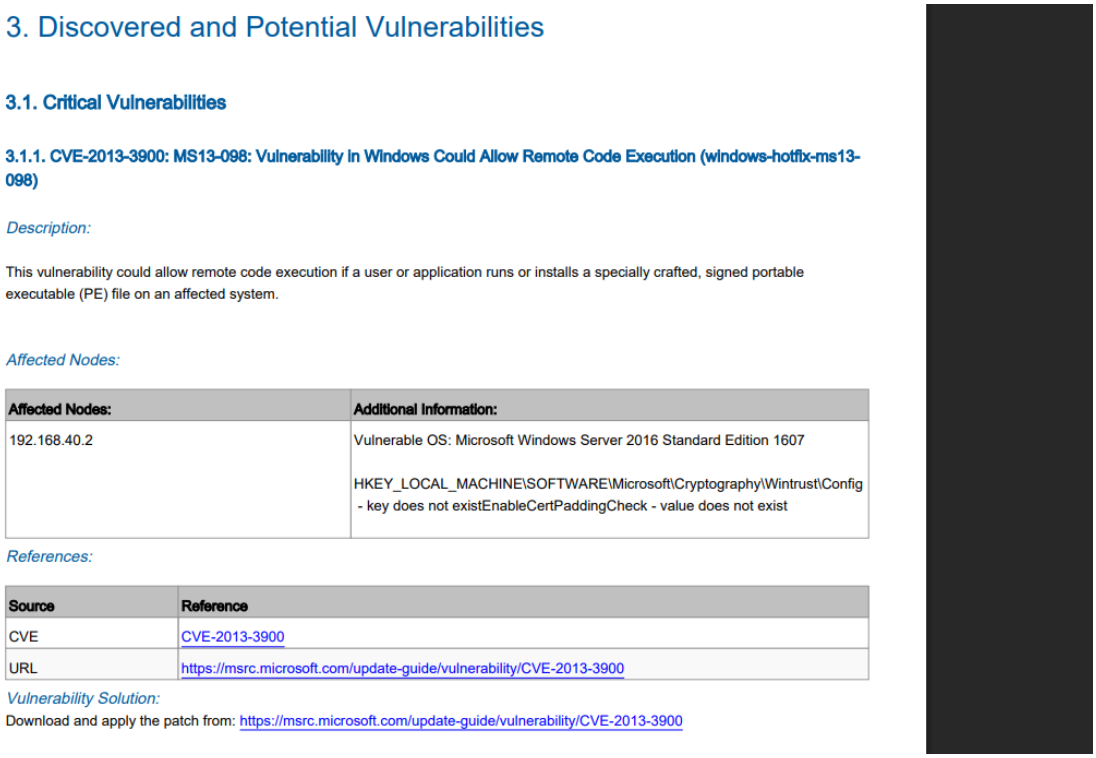
Kuva 15. Haavoittuvuuksien tarkistaminen manuaalisesti.

Haavoittuvuuksien korjaaminen

Haavoittuvuuksien korjaaminen on olennainen osa haavoittuvuuksien hallintaa. Haavoittuvuuksien korjaamiseksi asennetaan päivityksiä ja tarvittaessa tehdään kovennuksia päätelaitteille.

Seuraavaksi korjataan haavoittuvuus, joka on löydetty testiympäristön Windows Server 2016 -palvelimelta.

Korjaaminen kannattaa aloittaa ensin etsimällä kaikki palvelimelle saatavilla olevat päivitykset. Avataan ensin haavoittuvuusraportti, jossa on myös selitettynä toimenpiteet haavoittuvuuksien korjaamiseksi (Kuva 16).



3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. CVE-2013-3900: MS13-098: Vulnerability in Windows Could Allow Remote Code Execution (windows-hotfix-ms13-098)

Description:

This vulnerability could allow remote code execution if a user or application runs or installs a specially crafted, signed portable executable (PE) file on an affected system.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.40.2	Vulnerable OS: Microsoft Windows Server 2016 Standard Edition 1607 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Wintrust\Config - key does not existEnableCertPaddingCheck - value does not exist

References:

Source	Reference
CVE	CVE-2013-3900
URL	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

Vulnerability Solution:

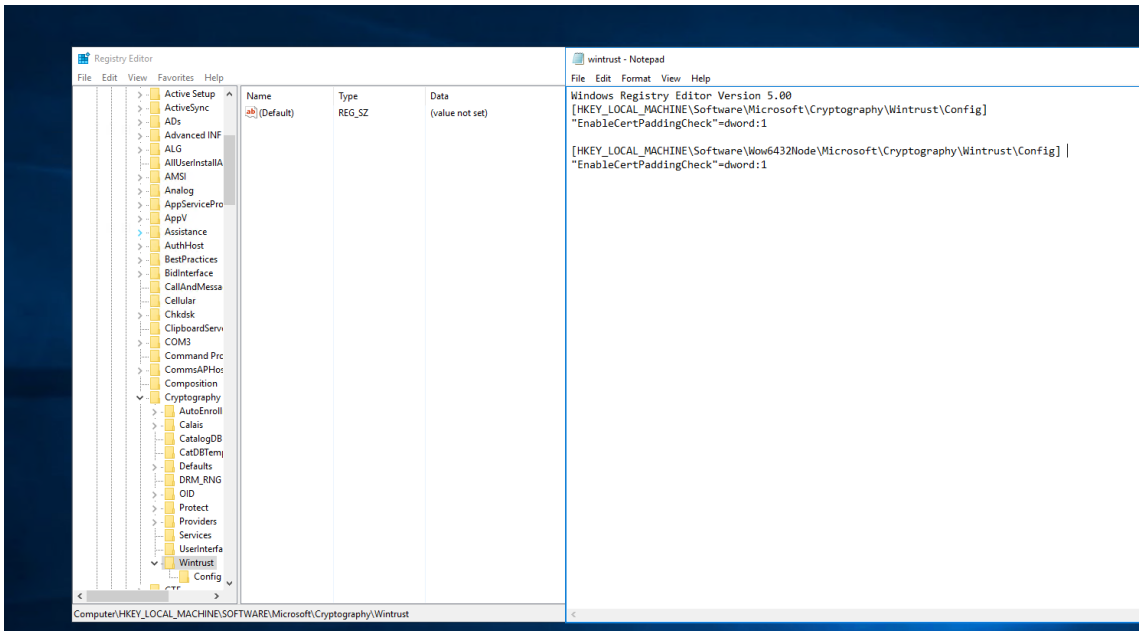
Download and apply the patch from: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

Kuva 16. Raportti palvelimen haavoittuvuuksista korjaustoimenpiteineen.

Testiympäristön palvelimelta löydetty ”Win Verify Trust Signature” on vakava tiedoston sähköisiin allekirjoituksiin liittyvä haavoittuvuus, jonka avulla hyökkääjä pystyy hyödyntämään haavoittuvuutta olemassa olevan tiedoston muokkauksessa lisäämällä haitallista koodia käytettäväksi. Käyttöjärjestelmä käyttää mekanismia tiedoston aitouden varmistamiseen mutta haavoittuvuuden vuoksi käyttöjärjestelmä ei välttämättä huomaa eroa allekirjoituksessa, joka mahdollistaa haitallisen koodin käyttämisen huomaamattomasti.

Haavoittuvuus korjataan kuvan 16 raportin mukaisesti Microsoftin nettisivuilta löytyvän ohjeen ja rekisteritietojen avulla. Valmis rekisteriteksti voidaan kopioida ja syöttää tekstin muokkausohjelmaan, joka tallennetaan palvelimen rekisteriin

(Kuva 17). Tämän jälkeen palvelin voidaan käynnistää uudestaan, jonka jälkeen haavoittuvuus on korjattu.



Kuva 17. Haavoittuvuuden korjaaminen rekisteritiedon lisäyksellä.