OULUN AMMATTIKORKEAKOULU

Janne Jaako

TIETOTURVAMÄÄRITTELY WINDOWS 2012 -PALVELIMEN INFRASTRUKTUURIPALVELUILLE

TIETOTURVAMÄÄRITTELY WINDOWS 2012 -PALVELIMEN INFRASTRUKTUURIPALVELUILLE

Janne Jaako
Opinnäytetyö
Kevät 2014
Tietojenkäsittelyn koulutusohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun seudun ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma, järjestelmäasiantuntemus

Tekijä:Janne Jaako
Opinnäytetyön nimi: Tietoturvamäärittely Windows 2012 palvelimen infrastruktuuripalveluille.
Työn ohjaaja: Kaisto Jukka
Työn valmistumislukukausi ja -vuosi: Kevät 2014 Sivumäärä: 37

Tämän opinnäytetyön aiheena on tietoturvan määrittely Windows 2012 infrastruktuuripalveluille. Toimeksiantajana toimi Oulun ammattikorkeakoulun it-palvelut, jonka palvelinympäristön tietoturvan tasontarkistaminen oli ajankohtainen käyttöympäristön päivittyessä Windows Server 2008R2:sta Windows Server 2012 käyttöympäristöön.

Opinnäytetyössä on selvitetty, nostaako Microsoftin määrittelemän tietoturvan tason saavuttaminen olennaisesti koko järjestelmän tietoturvaa. Opinnäytetyön pääasiallisena tietoperustana käytettiin Microsoftin TechNet-portaalia sekä alan kirjallista materiaalia. Palveluiden testaamiseen käytettiin MicrosoftHyper-V:llävirtualisoitua Microsoft Windows Server 2012:stamääriteltyjen palveluiden kanssa. Tietoturvariskien analysointiin käytettiin Windows- ja Linux-alustoille saatavia erikoisohjelmia. Tietoturvan tason määrittelyyn käytettiin Microsoftin SCM tool -, Baseline Analyzer - ja Microsoft SecurityAssessment -ohjelmia. Tuloksista tehtiin riskianalyysi vertaamalla testattujen riskien kykyä vahingoittaa järjestelmää niiden todennäköisyyteen tapahtua sekä niistä johtuviin vikatilanteisiin.

Työn lopputulokset on luovutettu Oulun ammattikorkeakoululle.Tulokset mahdollistavat järjestelmän tietoturvan tason nostamisen Microsoftin perustason yläpuolelle. Lisäksi ne auttavat sulkemaan tietoturva-aukkoja. Työssä asetetut tavoitteet saavutettiin.

Asiasanat: Windows Server, palvelut, tietoturva, riskianalyysi

ABSTRACT

Oulu University of Applied Sciences
Degree Program in Business Information Systems

Author :Janne Jaako
Title of thesis: Defining baseline security for Windows 2012 infrastructure services.
Supervisor :Kaisto Jukka
Term and year when thesis was submitted : Spring 2014 Pages: 37

The topic of this thesis is defining baseline security for Windows 2012 infrastructure services. This thesis was ordered by and made for Oulu University of Applied Sciences and its it-department. The need of baseline security testing was current because their server environment was updated from Windows Server 2008R2 to Windows Server 2012.

This thesis was made to examine if achieving the baseline defined by Microsoft would lead to better information security concerning the whole environment. Microsoft TechNet-portal and written material were used as a primary source for this thesis. Microsoft Windows Server 2012 with all the defined services was virtualized with Microsoft Hyper-V and used for the test environment. Windows- and Linux -platforms with special applications were used to test information security risks. Microsoft SCM tool, Baseline Analyzer and Microsoft Security Assessment programs were used to analyze the environment. The risk-analysis was made from the test outcome by comparing the ability of the risks to harm the system with their likelihood of occurring and with the results they can cause.

The results from the examination were given to theOulu University of Applied Sciences. The results will enable the information security level to be above Microsoft baseline. The results will also help to close down information security risks. The goals for this thesis were met.

Keywords: Windows Server, services, security, risk, analysis

SISÄLLYS

1 JOHDANTO 6
2 INFRASTRUKTUURIPALVELIMEN MÄÄRITTELEMINEN 8
2.1 Verkkoasetukset 8
2.2 Nimipalvelin 10
2.3 Toimialuepalvelin 13
3 PALVELUJEN TYYPILLISIMMÄT TIETOTURVARISKIT PALVELIMISSA 15
3.1 DHCP:n yleisesti tunnetut tietoturvariskit 15
3.2 Nimipalvelimen yleisesti tunnetut tietoturvariskit 17
3.3 Toimialuepalvelimen tietoturvariskit 18
4 KÄYTETYT OHJELMAT 20
4.1 Security ComplianceManager 3.0 20
4.2 Microsoft Security Baseline Analyzer 2.3 21
4.3 Microsoft Security Assessment 4.0 22
5 PERUSTASON ULKOPUOLELLE JÄÄVÄ JÄRJESTELMÄ 25
5.1 Riskien testaaminen käytännössä 25
6 PERUSTASOON PÄÄSSYT JÄRJESTELMÄ 27
7 RISKIANALYYSI 29
8 TULOKSET 31
9 JOHTOPÄÄTÖKSET 32
10 POHDINTA 33
11 LÄHTEET 35

1 JOHDANTO

Nykyinen tietoturva perustuu teknisiin ja organisatorisiin ratkaisuihin. Tietoturvan tekniset toimet perustuvat teknisiin sääntöperheisiin, protokolliin. Oikein tehdyt asetukset eivät kuitenkaan automaattisesti tarkoita aukotonta järjestelmää. Ne perustuvat sääntökokonaisuuksiin, joista osa on mahdollista kiertäätai rikkoa. Tyypillisen organisaation teknisen verkkostruktuurin tiedonvälitys ja -säilyttäminen rakentuu fyysisistä laitteista, koneista ja käyttäjistä. Verkon sisällä olevilla fyysisillä laitteilla hallitaan tiedonkulkua. Palvelimet tarjoavat toiminnot laitteiden keskinäiseen tiedonvälitykseen. Näitä perustoimintoja tarjoavia palvelimia voidaan kutsua infrastruktuuripalvelimiksi.

Tietoturvauhkien niin toivottu kuin tahatonkin havaitseminen on tehostanut niiden ehkäisemistä. Järjestelmät eivät kuitenkaan ole täydellisiä. Kehitettäessä yhä laajempia palvelinympäristöjä suuremmille asiakas- ja laitekokonaisuuksille tietoturvariskeiltä ei voida välttyä. Koska palveluilla on olemassa omat tunnetut riskinsä, niitä voidaan kuitenkin ennakoida ja hallita tarkastellessa laajentuvaa ja kehittyvää järjestelmäympäristöä. Yksi tekniikka tähän on tietoturvan perustasonsaavuttaminen. Perustasolla tarkoitetaan testattua tietoturvan tasoa, joka on saavutettavissa oikeilla päivityksillä, konfiguraatioilla ja verkon fyysisten laitteiden oikeilla asennuksilla.Perustason määritykset ovat osa toiminnallista riskienhallintaa.

Tietoturvan perustasolla (Baseline Security) tarkoitetaan yleisesti tietoturvalle tyypillisiä toimia ja prosesseja. Termiä voidaan käyttää eri yhteyksissä hieman eri tavalla laitevalmistajista, ohjelmistovalmistajista tai organisaatioista riippuen. Yleisesti tunnettuja perustasoja ovat esimerkiksi Microsoft Baseline Security,Cisco Security Baseline jaISO/IEC 27000. Näistä tässä opinnäytetyössä tarkastellaan Microsoftin määrittelemää perustasoa.

Yhteistä näille määrittelyille löytyy niiden kokonaisuuksista. Ne sisältävät kaikki tai joitain seuraavista osista: fyysisten laitteiden turvallisuus, päätelaitteiden turvallisuus, ohjelmien turvallisuus, käyttäjätilien valvonta, kulunvalvonta fyysisille laitteille, järjestelmän monitorointi ohjelmallisesti sekä automatisoituna, tietoturvakäytännöt ja riskien tiedostaminensekätietoturvaa tukevat prosessit (Microsoft Technet 2013. Hakupäivä 9.12.2013), (Cisco 2008. Hakupäivä 21.5.2014), (Information Security Standards 2011. Hakupäivä 21.5.2014). Organisaatio voi myös

määritellä oman perustasonsa joko itse tai mukailemalla jo olemassa olevia ratkaisumalleja. Yhteistä näille kaikille on kuitenkin se, että perustaso määrittelee ne toimet, joita noudattamalla päästään tietoturvamielessä tiettyyn pisteeseen.

Tässä lopputyössä tietoturvan perustasolla tarkoitetaan toimia ja konfiguraatioita, jotka *Microsoft* on määritellyt ratkaisemaan tietyn ongelman tai skenaarion määriteltyihin palveluihin liittyen. Käytännössä tämä tarkoittaa palveluiden asetuksia tietoturva huomioiden. Esimerkkinä tällaisesta perustasosta toimiioletusasetuksilla asennettukonfiguraatio ja suosituksen (bestpractise) mukainen määrittely. Microsoft tarjoaa oppaita ja ohjelmia Windows Server -tietoturvan perustason määrittämiselle palveluittain. Näiden välineiden ja ohjeiden tarkoitus on auttaa toteuttamaantehokas tietoturvan infrastruktuuri. Oikein toteutettuna perustason määrittämisellä pystytään ymmärtämään uhkia, valmistelemaan niille vastatoimia ja oppimaan palveluiden erikoisominaisuuksista (Microsoft Technet 2013. Hakupäivä 9.12.2013). Tässä lopputyössä tarkasteltiin Microsoftin suosituksia seuraaville Windows 2012 Serverin palveluille: DHCP, nimipalvelin ja toimialueohjain.

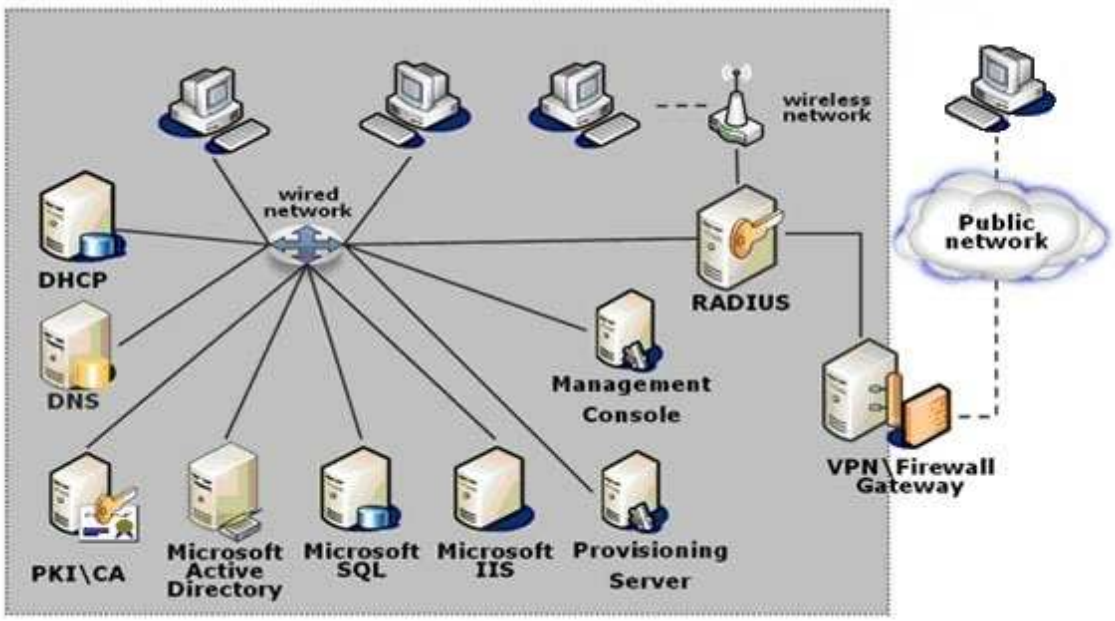
Opinnäytetyössä on selvitetty keskeisten palvelimien tietoturvan perustason määrittelyä Microsoftin mukaan. Teoreettinen osuus tarkastelitestattuja palveluita ja niiden tyypillisiä riskejäsekä ratkaisumalleja. Toiminnallisessa osassa asennettiin Windows Server 2012 Hyper-V-ympäristössä ja siihen otettiin käyttöön myös Oamk:n järjestelmässä toimivia palveluja. Palveluiden tunnettuja riskejä testattiin Microsoftin perustason ulkopuolelle jäävää sekä perustason saavuttanutta järjestelmää vastaan. Näitä kahta toteutusta verrattaessa sanotaanniitä tietoturvatasoiksi. Tietoturvan perustason saavuttanut järjestelmä määriteltiin testialustalle käyttäen Microsoftin SCM (Security ComplianceManager) tool -, Baseline Analyzer - ja Microsoft Security Assessment -ohjelmia.

Testattuja riskejä verrattiin riskianalyysissä. Riskien tason määrittämisessä otettiin huomioon niiden kyky vahingoittaa järjestelmää, todennäköisyys, vikatilanne ja kriittisyys. Riskit luokiteltiin asteikolla heikko, keskitasotai vakava.

Opinnäytetyön käytännön toteutukseen liittyvät testaukset sekä niistä saadut tulokset ovat toimeksiantajan pyynnöstä jätetty raportoimatta.

2 INFRASTRUKTUURIPALVELIMEN MÄÄRITTELEMINEN

Infrastruktuuripalvelimilla tarkoitetaan sellaisia palvelimia, joiden toiminnot ovat olennainen osa verkon kokonaisuutta ja sen tarjoamia palveluita. Verkon toiminta perustuu näiden verkon infrastruktuurille olennaisten palvelimien toimintaan (Kuvio 1) ja luo puitteet päätelaitteiden ja perustoimintojen hallitsemiseen. Infrastruktuuripalvelimia voidaan ajatella olevan ainakin DHCP, nimipalvelu, hakemistopalvelu, tulostuspalvelu, tiedostopalvelu, tietokantapalvelin, sertifikaattipalvelu, sovelluspalvelin (Web-palvelin), ryhmätyöpalvelin ja virtualisointipalvelu.



Kuvio1.Verkoninfrastruktuuri.(Waarith.Network infrastructure.Hakupäivä 29.5.2014)

2.1 Verkkoasetukset

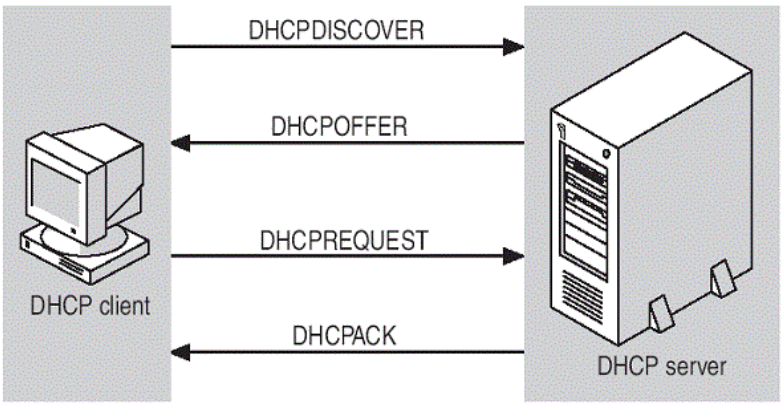
DHCP (DynamicHost Control Protocol) on verkkoprotokolla, jonka yleisin tehtävä on jakaa IP-asetuksia verkon laitteille (kuvio 1). Jaettavat osoiteavaruudet määritellään ylläpitäjän toimesta. Verkkoon kytkeytyessään laite pyytää DHCP-palvelimelta oman IP-osoitteensa. DHCP-palvelu kykenee jakamaan muitakin asetuksia. (Microsoft Technet 2003. Hakupäivä 18.12.2013).

TCP/IP -protokollaa käyttävissä tietokoneissa määritellään vähintään tietokoneen IP-osoite sekä aliverkon peite eli maski. Muita tavallisesti jaettavia tietoja ovat oletusyhdyskäytävä ja käytettävät nimipalvelimet. Jos näitä asetuksia ei ole määritelty tai ne on määritelty väärin, tietokone (tai muu päätelaite) ei toimi halutulla tavalla. Jaettuosoiteinformaatio on aliverkkokohtaista, jotense on uusittava siirrettäessä laitetta toiseen aliverkkoon. DHCP-palvelimen tehtävä on määritellä ja jakaa laitteiden TCP/IP- osoitteet automaattisesti (Kivimäki, J 2009. 601).

Käytännössä DHCP-palvelimella pystytään jakamaan lähes mitä tahansa verkkoasetuksia. Jaettu osoite on voimassa palvelimelta määritellyn elinajan (Time To Live, TTL). Menettely helpottaa päätelaitteiden hallintaa. DHCP-palveluita jakavia palvelimia voidaan sijoittaa samaan verkkoon useita, jolloin niiden kuormaa pystytään jakamaan. Samalla toimintavarmuus nousee. DHCP ei olereititttyvä protokolla, mutta se voi silti jakaa osoitteita toiseen verkkoon sallimalla DHCP Relay-toiminnonreitittimestä. Mikäli osoitepyyntö tulee toiselta verkkoalueelta, DHCP päättelee oletusyhteyskäytävän IP-osoitteesta verkkoalueen, josta osoite halutaan. (Microsoft Technet 2003. Hakupäivä 18.12.2013).

DHCP-palvelin on UDP/IP (User DatagramProtocol) protokollaan perustuvan perinteisen BOOTP-protokollan (Bootstrap-protocol) laajennus (IEFE 3396, 3442. Hakupäivä 29.5.2014), joka käyttääUDP-portteja67 ja 68. Kun DHCP-asiakas käynnistyy, se pyytää IP-osoitetiedot palvelimelta. Palvelimen vastaanottaessa pyynnön se valitsee IP-osoitetiedot tietokannassaan määritetystä osoitevarannosta (addresspool) ja tarjoaa tiedot asiakkaalle. Mikäli asiakas hyväksyy tarjouksen, DHCP-palvelinlainaa (lease) IP-osoitteen asiakkaalle tietyksi ajaksi (Kivimäki, J 2009. 601).

YksiDHCP-palvelin voi kontrolloida useita osoitealueita. Jaettavat osoitealueet ovat määriteltävissä erikseen ja niihin on mahdollista tehdä poikkeuksia. Jaettavista osoitteista on myös mahdollista eristää osoitteita pois. YksiDHCP-palvelin voi palvella sataakin tuhatta asiakasta ja hallita tuhatta osoitealuetta. Mitä enemmän palvelimella on asiakkaita, sitä tehokkaamman levyjärjestelmän palvelin tulee vaatimaan.Tietoturvan määrittelyn ja testaamisen kannalta olennaista on ymmärtää DHCP-palvelimen toiminta. Se helpottaa tunkeutujien työskentelyä: verkkoon pääsy on helppoa, jos verkosta saa automaattisesti oikein konfiguroidunIP-osoitteen (Kivimäki, J 2009. 601).



Kuvio2. DHCP-palvelimentoiminta. (Certshelp 2012. Hakupäivä 9.3.2014)

Asiakasohjelma lähettää DHCPDISCOVER-pyynnön sen liittyessä verkkoon. Tämä on UDP-paketti, jonka lähdeosoite on 0.0.0.0, kohdeosoite 255.255.255.255 ja porttinumero 67. KunDHCP-palvelin vastaanottaa tämän DHCPDISCOVER-pyynnön se vastaa DHCPOFFER-viestillä. Tämä tarjous sisältää asiakasohjelman pyytämän verkko-osoitteen/konfiguraation. Palvelin tallentaa asiakasohjelman MAC-osoitteenja sen yhteyden ip-osoitteeseen tietokantaansa osoittamaan tarjoamaansa osoitekonfiguraatiota. Osoite lähetetään takaisin palvelimelta porttiin 68. Kun paketti päätyy takaisin asiakasohjelmalle, se lähettää palvelimelle DHCPREQUEST-viestin. Tämä viesti ilmaisee, että osoitteen vastaanottaminen on hyväksytty. Viimeisenä vaiheena palvelin vastaanottaa DHCPPREQUEST-viestin ja lähettää DHCPPACK-viestin kertomaan asiakasohjelmalle, että sille on annettu oikeus IP-osoitteeseen (Anttila, A 2001. 202-218).

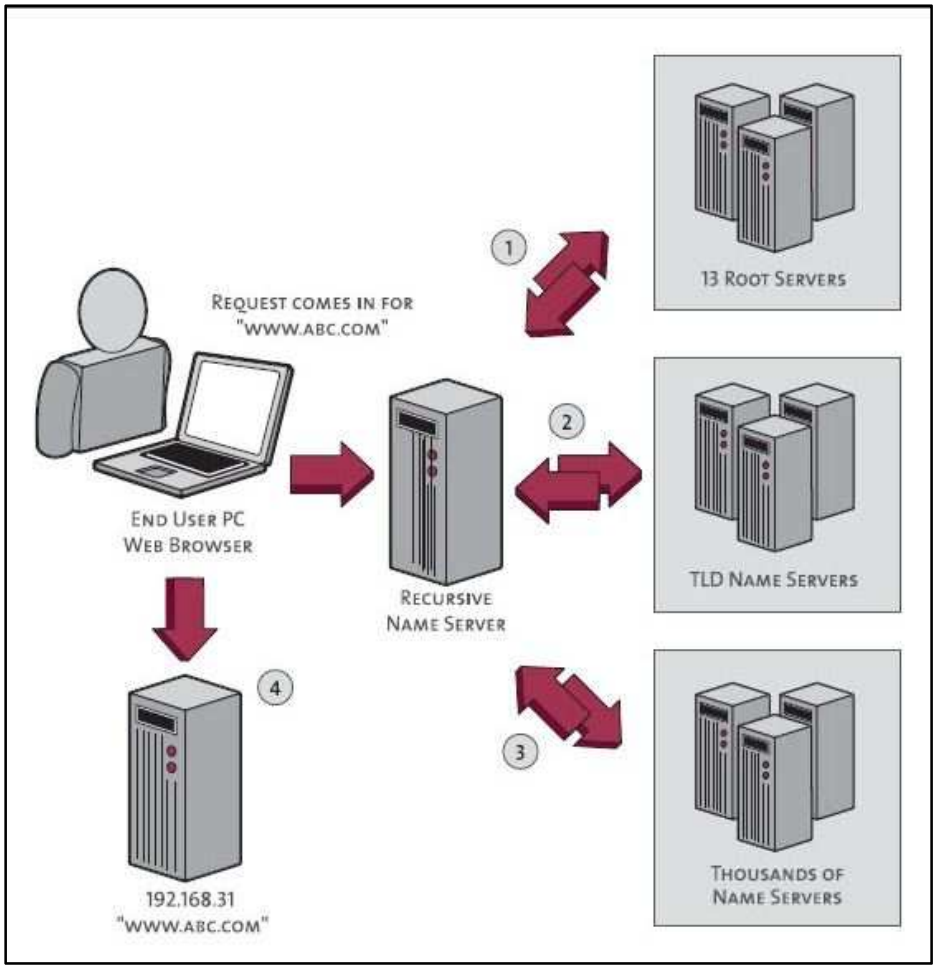
2.2 Nimipalvelin

1980-luvun alkupuolella jolloin nykyinen nimipalvelujärjestelmä esiteltiin, käytettiin tavallistahost-tekstitiedostoanimi-osoiteparien tallentamiseen. Vastaavan niminen host-tiedosto löytyy nykyisinkin lähes kaikilta käyttöjärjestelmiltä alustoista riippumatta. Se on tavallisesti vaihtoehtoinen keino nimiselvitykseen palvelimen puuttuessa. Koska hosts-tiedoston reaaliaikainen päivittäminen kasvoi mahdottomaksi tehtäväksi laitemäärän valtavan kasvun vuoksi, ongelma ratkaistiin nimiselvityspalvelimella. Perusajatuksena oli tarjota hajautetut hierarkiset nimi-palvelut sekä nimi- ja osoite- parien hallinta (RFC 1034, 1035). DNS-liikenne sisältää merkittävän osan globaalista verkkoliikenteestä. (Anttila, A 2001. 232).

Tietokoneista käytetään tavallisesti konenimiä, mutta Internet-protokollat käyttävät IP-osoitteita. Reititinverkon yhteyden muodostamiseksi tiettyyn kohteeseen IP-osoitteen avulla täytyy koneen nimeä käytettäessä selvittää sitä vastaava IP-osoite. Tätä sanotaan nimiselvitykseksi (Kuvio 3). Nimipalvelin selvittää IP-osoitetta vastaavan konenimen. Koska aktiivihakemiston toimialueet muodostavat nimeämisrakenteensa ja -hierarkiansa nimipalvelimen avulla, niin aktiivihakemisto liittyy tiiviisti nimipalvelimen käyttöön.

Kun nimipalvelin otetaan käyttöön, on määriteltävä nimipalvelua tarjoavat palvelimet sekä sitä käyttävät asiakkaat. Asiakaskoneille konfiguroidaan nimipalvelinten osoitteet (IPv4, IPv6). Sen jälkeen asiakkaat voivat kommunikoida nimipalvelimen kanssa, vaikka ne sijaitsisivat eri verkoissa. (Kivimäki 2009, 473).

Asiakkaan pyytäessäIP-osoitetta se lähettää suoran kyselyn (forwardlookupquery) paikalliselle nimipalvelimelle. Nimipalvelin ratkaisee kyselyn tietokantahaulla ja palauttaa asiakkaalle vastauksen. Mikäli nimipalvelimen tietokannasta ei löydy vastausta kyselyyn, se lähettää kyselyn edelleen juuripalvelimelle. Tätä hierarkiaa pyöritetään niin kauan kunnes haluttu osoite löytyy mikäli sellainen on olemassa. Kyselyn voi suorittaa IP-osoitteesta nimeksi tai toisinpäin. Nimipalvelimen toinen tehtävä on sähköpostin reititys (Kivimäki 2009, 478).



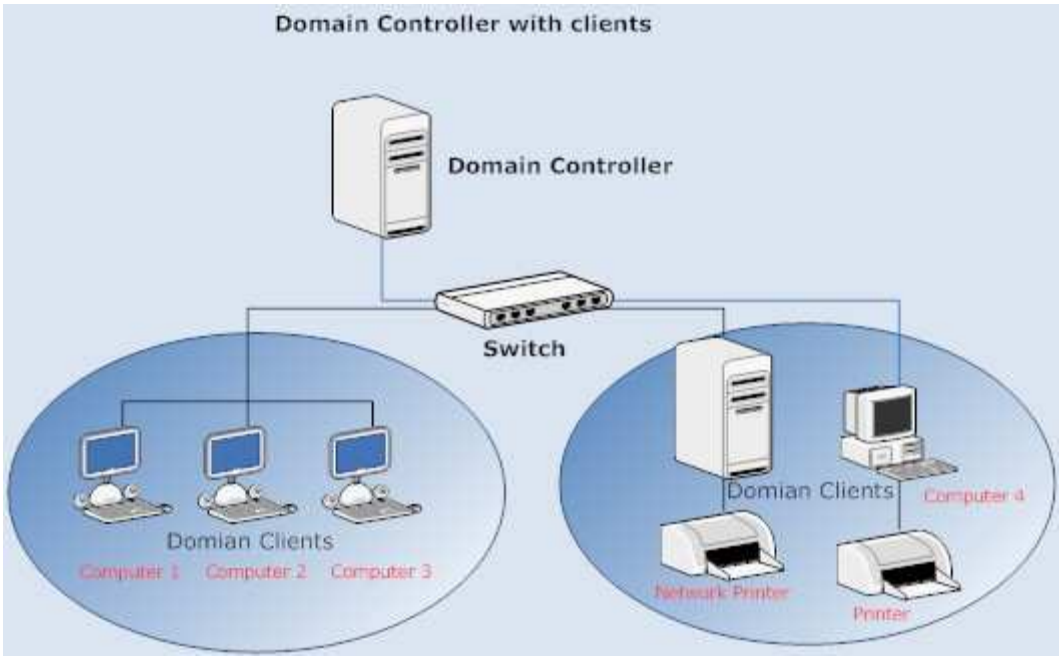
Kuvio 3. Nimipalvelimen toiminta.(Spiceworks 2009. Hakupäivä 9.3.2014.)

Nimipalvelukyselyihin vastauksia hakevia koneita sanotaan nimipalveluohjelmistoiksi(resolver). Vastauksia antavia koneitakutsutaanepä-auktoratiivisiksi ja auktoratiivisiksi nimipalvelimiksi. Normaalisti nimipalvelimella tarkoitetaan ainoastaan resolveria, joka määritellään verkon koneille staattisesti tai DHCP:n avulla. Tavallisesti niitä määritellään kaksi tai useampia. Useamman resolverin käyttö parantaa vikasietoisuutta. Mikäli ensisijainen nimipalvelin lopettaa toimintansa,pysyy toissijainenresolveri toiminnassa. Toinen resolveri mahdollistaa myös kuorman tasaamisen (TCP/IP guide. 2005. Hakupäivä 29.5.2014). Resolveri etsii vastauksia nimipalvelukyselyihin. Ne tallettavat vastauksia välimuistiin, millä vältetään rekursio silloin, kun nimeä tarvitaan uudelleen. Resolverin rekursio tarkistaa, onko kysytty nimi välimuistissa. Jos nimi on välimuistissa, eikä se ole vanhentunut, palautetaan se ilman rekursiota. Mikäli vain nimen vähemmän merkitsevä osa on välimuistissa, tehdään ulossuuntautuvia kyselyitä nimen selvittämiseksi. Jos välimuisti on tyhjä, resolveri käyttää tietoajuuripalvelimista löytääkseen

osoitteen nimelle. Välimuistin elinaikaa määritelläänTTL-mekanismilla (Time-To-Live). Auktoratiivisillä nimipalvelimet vastaavatresolvereidenkyselypyyntöihin. Toimialueen suhteen vähemmän merkitsevät nimipalvelimet kuten juurinimipalvelimet eivät tiedä lopullista vastausta. Ne kuitenkin tietävät reitin enemmän merkitsevämmälle nimipalvelimelle, josta tieto todennäköisimmin löytyy.

2.3 Toimialuepalvelin

Toimialueohjain valvoo toimialueeseen kuuluvien tietokoneiden käyttöoikeuksia. Se vastaa tilien tiedoista, autentikoinnista ja istunnoista sekä valvoo toimialueen tietoturvakäytäntöjä. Toimialueohjain valvoo toimialueen palvelujen resursseihin pääsyä (Kuvio 4).



Kuvio4. Toimialueohjain verkossa. (Scientificera 2012. Hakupäivä 29.5.2014)

Toimialue termillä tarkoitetaan eri asiaa nimipalvelun ja aktiivihakemiston yhteydessä. Aktiivihakemiston yhteydessä toimialueella tarkoitetaan tietokoneista, työasemista, käyttäjätileistä, ohjelmistoista ja muista laitteista muodostunutta kokonaisuutta, jota hallitaan yhtenä yksikkönä. Laitteet voivat olla eri verkoissa ja niihin voi olla liittyneenä tuhansia hallittavia objekteja. Aktiivihakemiston kannalta toimialue on hakemistotietokannan yksi osio, jota toimialueen ohjauspalvelimet ylläpitävät (Kivimäki 2009, 479). Aktiivihakemistojen toimialueiden

nimeämiskäytännöt ja hierarkiat muistuttavat hyvin paljon nimipalvelun nimeämissääntöjä. Aktiivihakemiston nimi on samalla myös nimipalvelun toimialueen nimi.

Samalla toimialueella voi olla monta toimialueohjainta. Tämä vähentää yhteen ohjaimeen kohdistuvaa kuormaa. Useampi ohjain mahdollistaa myös replikoinnin ja parantaa autentikoinnin toimintavarmuutta. Mikäli yksi kahdesta tai useammasta toimialueohjaimesta poistetaan verkosta, muut vastaavat, yleensä replikoivat ohjaimet, pystyvät korvaamaan poistuneen ohjaimen roolin.

3 PALVELUJEN TYYPILLISIMMÄT TIETOTURVARISKIT PALVELIMISSA

Kaikki palvelimiensisältämät palvelut ovat tietoturvariski. Palveluiden riskit ovat pääsääntöisesti samat riippumatta niiden palvelunsisällöstä. Pääasiallisia riskejä ovat autentikointiin liittyvät todennukset, palvelunestohyökkäykset, ylivuotaminen, erilaiset ohitusmetodit, tiedon urkkiminen, vahingollisen koodin ajaminen, muistivirheet jne. Koska riskejä on paljon, on niiden tunnistaminen välttämätöntä.

Järjestelmän tietoturvaheikkouksista tulee olla ajantasalla. Windows-palvelinten sekä työasemien heikkouksien etsiminen kannattaa aloittaa etsimällä jo löydettyjä tunnettuja tietoturva-aukkoja. Palomuurin ulkopuolelta tapahtuvien verkkomurtojen havaitsemisen päämääränä on auttaa organisaatiota vastaan suunnattujen hyökkäysten arvioinnissa ja, että sisäiset palvelut on kovetettu näitä hyökkäyksiä vastaan(Noarthcutt S, Novak J. 2002, 460).

Tietoturva-aukkojen ja päivitysten seurantaan ei välttämättä tarvita erillistä prosessia, mutta sen seuranta tulee vastuuttaa tietylle taholle. Lisäksi kannattaa miettiä niitä tietolähteitä, joita seurataan. Esimerkiksi järjestelmä ja -ohjelmantoimittajien postituslistat ja RSS-lähteet, CERT-listat ja virustorjuntasovellusten toimittajen virusraportit ovat tällaisia tietolähteitä (Laaksonen, Nevasalo, Tomula 2006, 156). Yksi niistä on CVEDetails -yrityksen ylläpitämä cvedetails.com -sivusto. Palvelu auttaa hahmottamaan infrastruktuurin riskejä ja korjaamaan niitä.

3.1 DHCP:n yleisesti tunnetut tietoturvariskit

DHCP-protokolla ei sisällä autentikointimekanismeja, joten se on varsin haavoittuva hyökkäyksille. Tyypillisimpiä näistä ovat auktorisoimattomien asiakkaiden pääsy verkkoresursseihin, auktorisoimattomien DHCP-palvelimien väärän tiedon jakaminen verkkoon ja DHCP-palvelimen tukehduttaminen olemattomilla asiakastietokoneilla resurssien osoitteiden tukkimiseksi. Hyökkäys voidaan toteuttaa usealla eri tavalla.

Päätelaitteen on mahdotonta tunnistaa DHCP-palvelimen oikeellisuutta ja näin auktorisoimatonDHCP-palvelin voi aiheuttaa *DoS*(Denial of Service) -tilanteentahattomastikin. Koska DHCP voi jakaa IP-osoitteidenmukana muuta osoite-informaatiota, kuten nimipalvelimen

osoitteen, voidaan sitä käyttää myös *man-in-the-middle* hyökkäykseen. Väärästä DHCP-palvelimesta annettu väärennetty nimipalvelimen osoite mahdollistaa liikenteen ohjaamisen mihin tahansa. Lisäksi väärennetyn nimipalvelimen kautta kulkeva informaatio pystytään lukemaan. Päätelaitteita (asiakasohjelmia) voidaan myös pyytää ottamaan uusia osoitteita jatkuvasti väärentämällä paketteja ja näinkuluttaa pooli loppuun. Saatuja tietojanapatuista osoitteista ja niiden sisältämästä tiedosta voidaan myös hyödyntää myöhemmin tapahtuvassa hyökkäyksessä. (The TCP/IP Guide 2005. Hakupäivä 18.12.2013).

Tätä opinnäytetyötä varten virtuaalialustalla tehdyssä esimerkkihyökkäykesssäDHCP-palvelintavastaan saatiin aikaiseksi tila, jossa poolin osoitteet kulutettiin loppuun (DoS-hyökkäys). Se aiheuttaa käyttökatkon muiden asiakkaiden pyynnöille. Ensimmäisessä vaiheessa hyökkääjä lähettää DHCPDISCOVER-pyyntöjä palvelimelle.Mitä useammasta lähteestä pyyntöjä lähetetään, sitä suurempi onpalvelimelle aiheutunut roskakuorma. On huomattava, että roskakuorman lähteitä voi olla periaatteessa äärettömästi. DHCP-pyyntöjä on varsin tehokasta lähettää. Paketteja on nopea generoida ja jo muutaman sekunnin ajo tuottaa kymmeniätuhansia pyyntöjä (testiympäristössä 15000-40000 pyyntöä). DHCPDISCOVER-pyyntöjen toteuttamiseen on useita tapoja. DHCP-palvelin vastaa kyselyyn DHCPOFFER-viestillä kunnes koko osoiteavaruus on käytetty.

Toinen testattu esimerkki on käyttää hyökkäystä sekä DoS-hyökkäykseen, että tiedon keräämiseen. Aluksi kerättiin verkosta tietoa. Tärkeimpiin tietoihin kuuluu mikä tahansa saatu IP-osoite, nimipalvelimen tiedot ja defaultgateway. Tämän jälkeen verkkoon tuodaan uusi DHCP-palvelin, jolle asetetaan selvitetty osoiteavaruus. Alkuperäistä osoiteavaruutta voi simuloida tarkasti. Kun tämä toinen DHCP-palvelin tuodaan käyttöön, se jakaa osoitteita antaen väärennetty' tietoa DoS-hyökkäyksenä. Koska DHCP-palvelin voi jakaa myös muutakonfiguraatiotietoa, sen myrkyttämien päätelaitteiden tieto voidaan lukea ja liikenne ohjata haluttuun esimerkiksi väärennettyyn osoitteeseen.

3.2 Nimipalvelimen yleisesti tunnetut tietoturvariskit

Nimipalvelun tietoturvaongelmia ovat välimuistin väärentäminen, tulviminen (flooding, DoS-hyökkäys) ja kalastelu. Nimipalvelin saa tietonsa kyselytuloksina muilta nimipalvelimilta ja tallentaa tiedot niiden nopeampaa käsittelyä varten välimuistiin (DNS-cache). Nimipalvelua ei kiinnosta, mitä muualta tulleessa vastauksessa on sisältönä ollenkaan. Eli www.esimerkki.fi:n vaihtuminen www.esimerkk1.fi:ksinimipalvelimen välimuistissaei kiinnostanimipalvelinta. Tällaisesta väärää nimipalvelin tietoa levittävästä hyökkäyksestä käytetään nimitystä "välimuistin myrkyttäminen". Saman lopputuloksen saa aikaan asiakkaan host-tiedoston väärentämiselläpaikallisesta koneesta polustac:\windows\system32\drivers\etc. Tarkistamaton tieto aiheuttaa nimen ohjaamisen väärennettyyn osoitteeseen.

Tulviminen tarkoittaa tässä yhteydessä nimipalvelun tukkimista pyynnöillä. Tämä on palvelunesto, jolloin nimipalvelinlopettaa vastaamisen sitä käyttäville "oikeille asiakkaille" (WindowsSecurity.com 2011. Hakupäivä 28.4.2014). Nimipalvelimen palveluneston toteuttaminen on yksinkertaista, koska nimipalvelin, kuten DHCP-palvelukaan, ei vaadi autentikointia. Se yrittää vastata kaikille sille lähetetyille pyynnöille niiden määrästä riippumatta. Nimipalvelinta kohtaan automatisoivia hyökkäysohjelmistoja on paljon ja niiden käyttäminen on yksinkertaista. Pelkkä palvelunesto kuitenkin yhdistetään yleensä nimipalvelun uudelleenohjaukseen ja verkkokalasteluun.

Kun nimipalvelin on saatu palvelunestotilaan, voidaan verkkoon tuoda valvomaton nimipalvelin (rogue-server). Sen tunnistaminen verkkoanalysaattoreilla on ylläpitäjän puolelta mahdollista, mutta se voi jakaa verkkoon virheellistä tietoa.

Ennen tätä virheellinen sivusto on tietenkin pitänyt luoda. Koska verkkosivujen graafisen ilmeen samankaltainen luominen on yksinkertaista, voi loppukäyttäjän olla hankala huomata siirtymistä / ohjaamista väärälle sivustolle. Tämän jälkeen loppukäyttäjän väärälle sivustolle antama data kerätään talteen ja käytetään toisin. Tällaista käyttäjien ohjaamista väärälle sivustolle ja sitä kauttakerättyä tietoa sanotaan kalasteluksi (Securelist. Hakupäivä 28.4.2014).
Tavallisesti väärennettyä tietoa on helpoin etsiä seuraamalla normaalia korkeampia TTL-aikoja.

3.3 Toimialuepalvelimen tietoturvariskit

Verkkotoimialueohjaimen pääasiallisina riskeinä ovat autentikoidut salasana hyökkäykset (pass the hash) sekä palvelunestohyökkäykset. Autentikoidulla salasanahyökkäyksellä tarkoitetaan tässä yhteydessä sellaista murtautumistekniikkaa, jossa hyökkääjän ei tarvitse autentikoitua ollenkaan perinteisellä tunnetulla salasanalla. Hyökkääjä voi käyttää NTLM- tai LanManhash-jälkeä, joka on jäänyt joltain autentikoituneelta käyttäjältä. Kunkäyttäjänimistä ja salasanoista ollaansaatuhash, voidaan niitä käyttääautentikointiin ilman, että hash-tietoaavataan ohjelmallisesti murtamalla. Ohjelmallista murtamista voidaan edelleen kylläkäyttää ja nykyisellä koneteholla se on yllättävän nopeaa salauksesta ja salasanan pituudesta riippumatta. Salausta purettaessa on huomattavasti tehokkaampaa käyttää koneen näytönohjaintaprosessorilla laskemisen sijaan. Mikäli salauksen purkaminen paikallisella vie liian pitkään, voi netistä ostaa suoraaanhash-purkamiseen tarvittavaa konetehoa.

Windowsin käyttäjän hash-tietoja tallentaa SAM-tietokanta, johon kaikillapaikalliseenadministrator-ryhmäänkuuluvilla on oikeus. Mikäli asiakaskoneella on paikallinen administrator-ryhmään kuuluva tunnus (tai ryhmään automaattisesti kuuluvaa perusasennuksessa luotua tunnusta on käytetty), on mahdollista käyttää olemassa olevaa hash-jälkeä tunnustautumiseen sen jälkeen, kun asiakaskoneelle on jo kirjauduttu. Tämä tapahtuu kolmannen osapuolen pass-the-hash-ohjelmalla. Niitä on useita. Ohjelmat mahdollistavat paikallisen tunnistautumisen,LSA:n(Local Security Authority), käyttämän käyttäjänimen, verkkoalueen ja salasanan hash-tiedon vaihdon ajon aikana sen jälkeen, kun ollaan jo autentikoiduttu (BasharEwaida 2010. Hakupäivä 28.4.2014).

Palvelunestohyökäykkäystoimialueohjaimeen voi tapahtuamyös epäsuorasti, mikäli toimialueohjain on asennettu niin, että PDC:n (PrimaryDomain Controller) kanssa on asennettu joukko tarpeettomia protokollia ja palveluita. Tämä on parhaiden suositusten vastainen asennusvirhe ja on korjattavissa noudattamalla hyväksi havaittuja käytäntöjä. (SANS Institute 2000-2002. Hakupäivä 29.5.2014) Toimialueohjaimeen kohdistuu myös muita heikkouksia.Esimerkiksi toimialueohjaimenLDAP-hakemistopalvelun protokolla on herkkä palvelunestohyökkäyksille. (CVE-Details 2013. Hakupäivä 6.5.2014). Mikäli palvelu on käynnissä, siinä olevia heikkouksia voidaan käyttää hyväksi. Windows palvelin 2012 sisältää myös useita sertifikaattiväärennöksiin liittyviä heikkouksia. Myös näitä sertifikaattiväärennöksiin

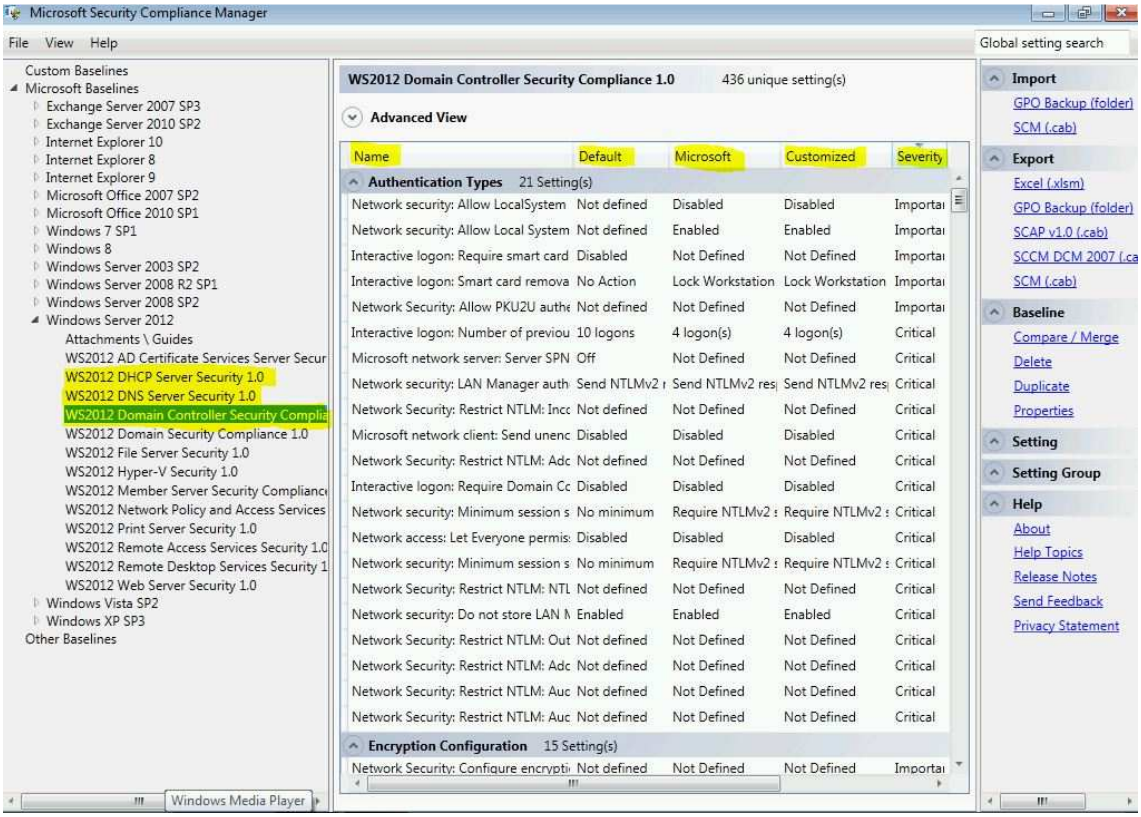
liittyviäheikkouksia voidaan käyttää toimialueohjaimen kaatamiseksi. (CVE-Details 2013. Hakupäivä 6.5.2014)

4 KÄYTETYT OHJELMAT

Tietoturvan perustason määrittämisen työkaluina käytettiin Microsoftin tietoturvan sisäisen valvonnan hallinnointiohjelmaaSCM (Security ComplianceManager) 3.0 (Kuvio 5), tietoturvan perustason analysointiohjelmistoa MBSA (Microsoft Baseline Security Analyzer) 2.3 Kuvio 6, sekä Microsoftin tietoturvan arviointiohjelmaa MSA (Microsoft Security Assessment) 4.0 (kuvio 7, kuvio 8)-ohjelmia. Ohjelmien toiminta perustuu verkon tilan analysointiin ja hyvien tunnettujen käytäntöjen käyttöönoton ohjeistamiseen. Ohjelmat antavat myös tietoa päivityspakettien tilanteesta.

4.1 Security ComplianceManager 3.0

SCM mahdollistaa konfiguroinnin ja hallinnoinnin tietokoneille käyttämällä ryhmäkäytäntöjä sekä SCCM:ää (ei käytössä testiympäristössä).

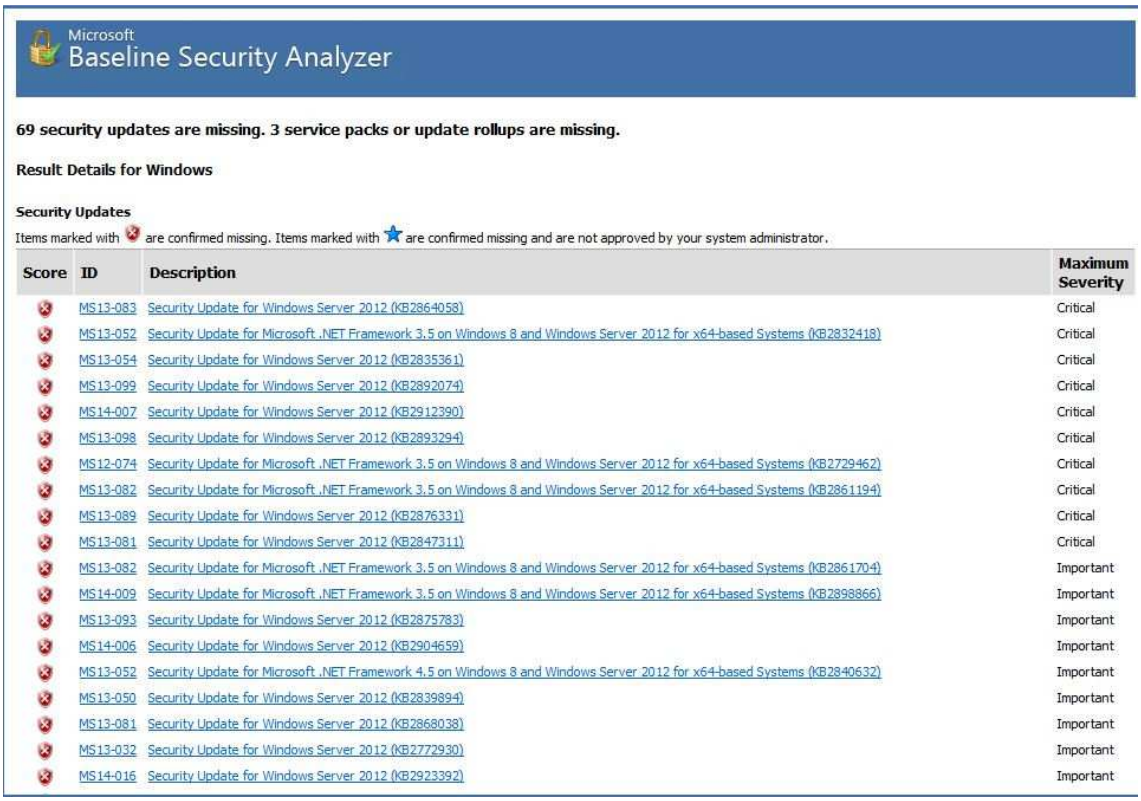


Kuvio5. Security ComplianceManager 3.0

SCM 3.0 tukee valmiita käytänteitä sekä konfigurointipaketteja perustuen parhaisiin käytänteisiin. Se kertoo kuinka vakavasta riskistäkonfiguraatiossa on kyse ja mikä on sen perusasennus suositukseen verrattuna.SCM-ohjelmistoncab-tiedoston sisältämistä Windows 2012-käyttöjärjestelmän komponenteista on tässä työssä käytetty seuraavia: WS2012 DHCP Server Security 1.0, WS2012 DNS Server Security 1.0, WS2012 Domain Controller Security Compliance 1.0 (Microsoft Technet.Hakupäivä 6.5.2014).

4.2 Microsoft Security Baseline Analyzer 2.3

MBSA-ohjelma tarkistaa järjestelmän turvallisuustilan. Se osaa verrata saatavilla oleviin päivityksiin,onko järjestelmässä varmasti viimeisimmät päivitykset ja ovatko tietoturvaan liittyvät asetukset kunnossa. MBSA osaa esimerkiksi varoittaa, jos paikalliset salasanat ovat liian heikkoja tai Windowsin palomuuriin on vahingossa avattu turhia reikiä.MBSA-ohjelmaosaa järjestelmän lisäksi tutkia ja varoittaa myös Microsoftin omien palvelinohjelmistojen uhkia muodostavista vääristä asetuksista.



Microsoft Baseline Security Analyzer

69 security updates are missing. 3 service packs or update rollups are missing.

Result Details for Windows

Security Updates

Items marked with are confirmed missing. Items marked with are confirmed missing and are not approved by your system administrator.

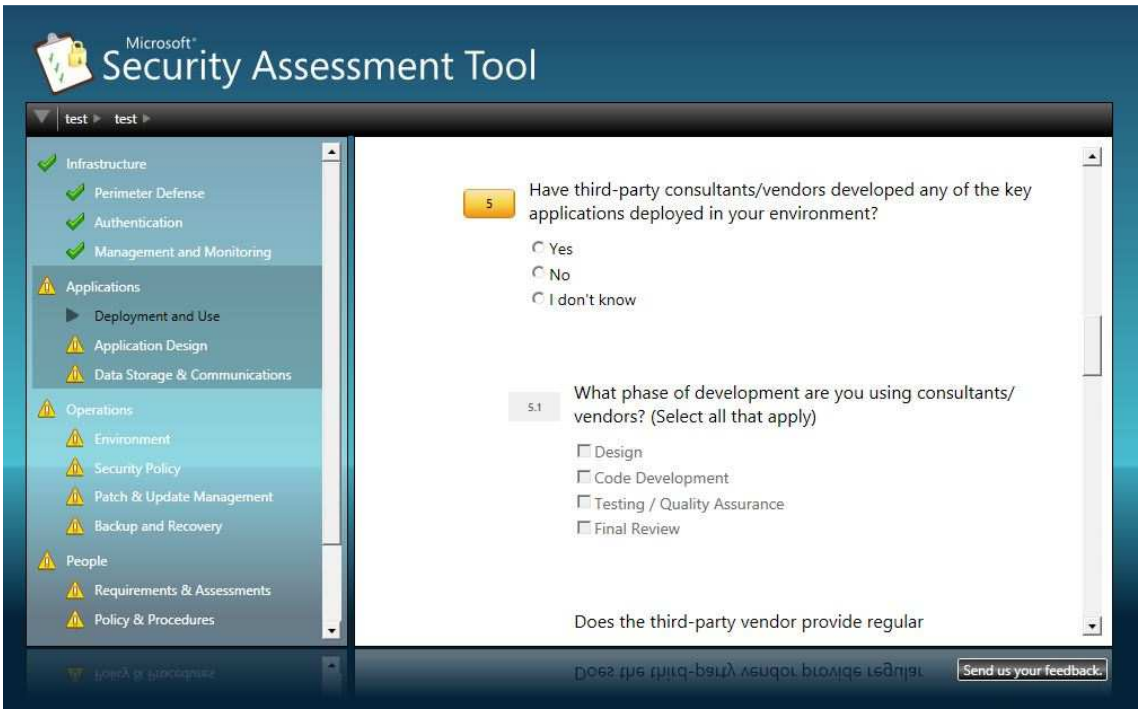
Score	ID	Description	Maximum Severity
	MS13-083	Security Update for Windows Server 2012 (KB2864058)	Critical
	MS13-052	Security Update for Microsoft .NET Framework 3.5 on Windows 8 and Windows Server 2012 for x64-based Systems (KB2832418)	Critical
	MS13-054	Security Update for Windows Server 2012 (KB2835361)	Critical
	MS13-099	Security Update for Windows Server 2012 (KB2892074)	Critical
	MS14-007	Security Update for Windows Server 2012 (KB2912390)	Critical
	MS13-098	Security Update for Windows Server 2012 (KB2893294)	Critical
	MS12-074	Security Update for Microsoft .NET Framework 3.5 on Windows 8 and Windows Server 2012 for x64-based Systems (KB2729462)	Critical
	MS13-082	Security Update for Microsoft .NET Framework 3.5 on Windows 8 and Windows Server 2012 for x64-based Systems (KB2861194)	Critical
	MS13-089	Security Update for Windows Server 2012 (KB2876331)	Critical
	MS13-081	Security Update for Windows Server 2012 (KB2847311)	Critical
	MS13-082	Security Update for Microsoft .NET Framework 3.5 on Windows 8 and Windows Server 2012 for x64-based Systems (KB2861704)	Important
	MS14-009	Security Update for Microsoft .NET Framework 3.5 on Windows 8 and Windows Server 2012 for x64-based Systems (KB2898866)	Important
	MS13-093	Security Update for Windows Server 2012 (KB2875783)	Important
	MS14-006	Security Update for Windows Server 2012 (KB2904659)	Important
	MS13-052	Security Update for Microsoft .NET Framework 4.5 on Windows 8 and Windows Server 2012 for x64-based Systems (KB2840632)	Important
	MS13-050	Security Update for Windows Server 2012 (KB2839894)	Important
	MS13-081	Security Update for Windows Server 2012 (KB2868038)	Important
	MS13-032	Security Update for Windows Server 2012 (KB2772930)	Important
	MS14-016	Security Update for Windows Server 2012 (KB2923392)	Important

Kuvio6. MBSA:n esimerkkitulos

Mikäli ohjelma löytää järjestelmästä tietoturvaa heikentäviä asetuksia tai vanhoja ohjelmistoversioita, se huomauttaa niistä käyttäjälle tarkastuksen lopuksi. Käyttäjä saa myös raportin järjestelmän tilasta. Ilmoituksessa on usein myös suora linkki tarvittavaan päivitykseen tai asetusten korjaamisessa helpottavaan Microsoft Knowledge Base -artikkeliin (Pitkänen 2008, Hakupäivä 1.10.2014).

4.3 Microsoft Security Assessment 4.0

Microsoft Security Assessment on uusittu ohjelmaversioMicrosoft Security Risk-itsearviointityökalusta (MSRSAT). Työkalu käyttää kokonaisvaltaista turvallisuusmittausta yhdistämällä eri prosesseja ja teknologioita. Tuloksiin vaikutetaan vastaamalla MSA:n kyselyyn organisaatiorakenteesta, tietoturvasta jainfrastruktuurikokonaisuudesta. Tämä informaatio antaa tavallisesti tarkat tiedot ja metodit havaitun riskin minimoimiseksi oikein. Nämä tiedot sisältävät työkaluja ja parhaiden käytänteiden oppaita.



Kuvio 7. Tiedon syöttäminen MSA:han

MSA sisältää kaksi työkalua:

- Business Risk Profile Assessment
- Defense in Depth Assessment

Kuvio8. MSA:n ohjeita sinne syötetyn tiedon perusteella

Järjestelmän tilan konfiguraatiotieto annetaan vastauksenaMSA:n kyselyyn, joka liittää sen suositeltavan käytännön mukaisiin turvallisuustoimintoihin riippumatta siitä, ovatko niiden vaatimat toimet peruskonfiguraatiossa vai vaativatko ne erikois-toimenpiteitä. Tulokset perustuvat 17799 ja NIST-800.x ISO-standardeihin sekä Microsoftin luotettavaksi tunnustamiin yhteistyökumppaneihin tietoturvan alalla. MSA:n ohjelmisto on ilmainen ja saatavilla Microsoftin sivustolta tuetuille alustoille (Microsoft 2012. Hakupäivä 6.5.2014).

5 PERUSTASON ULKOPUOLELLE JÄÄVÄ JÄRJESTELMÄ

Perustason ulkopuolelle jäävää järjestelmää vastasi oletusasetuksilla asennettu ja päivittämätön Windows 2012 Server -palvelinympäristö. Siihen oli asennettu vain testattavat palvelutsekä testausohjelmistoja. Koska perustasoa ei saavutettu, sen tietoturvassa oli heikkouksia.

5.1 Riskien testaaminen käytännössä

Riskien testaaminen toteutettiin aina samalla tavalla. Ensimmäisenä haettiin tietoa tunnetuista riskeistä tarkasteltavalle palvelulle. Tämän jälkeen etsittiin, onko hyväksikäytettävässä tietoturvariskissä jo olemassa olevaa korjausta ja mikäli näin on niin, onko se jo asennettu. Itse testaamisen toteuttamiseen käytettiin valmiita työkaluja, joita ajettiin pääsääntöisesti Linuxin käyttöjärjestelmäjakeluilla.

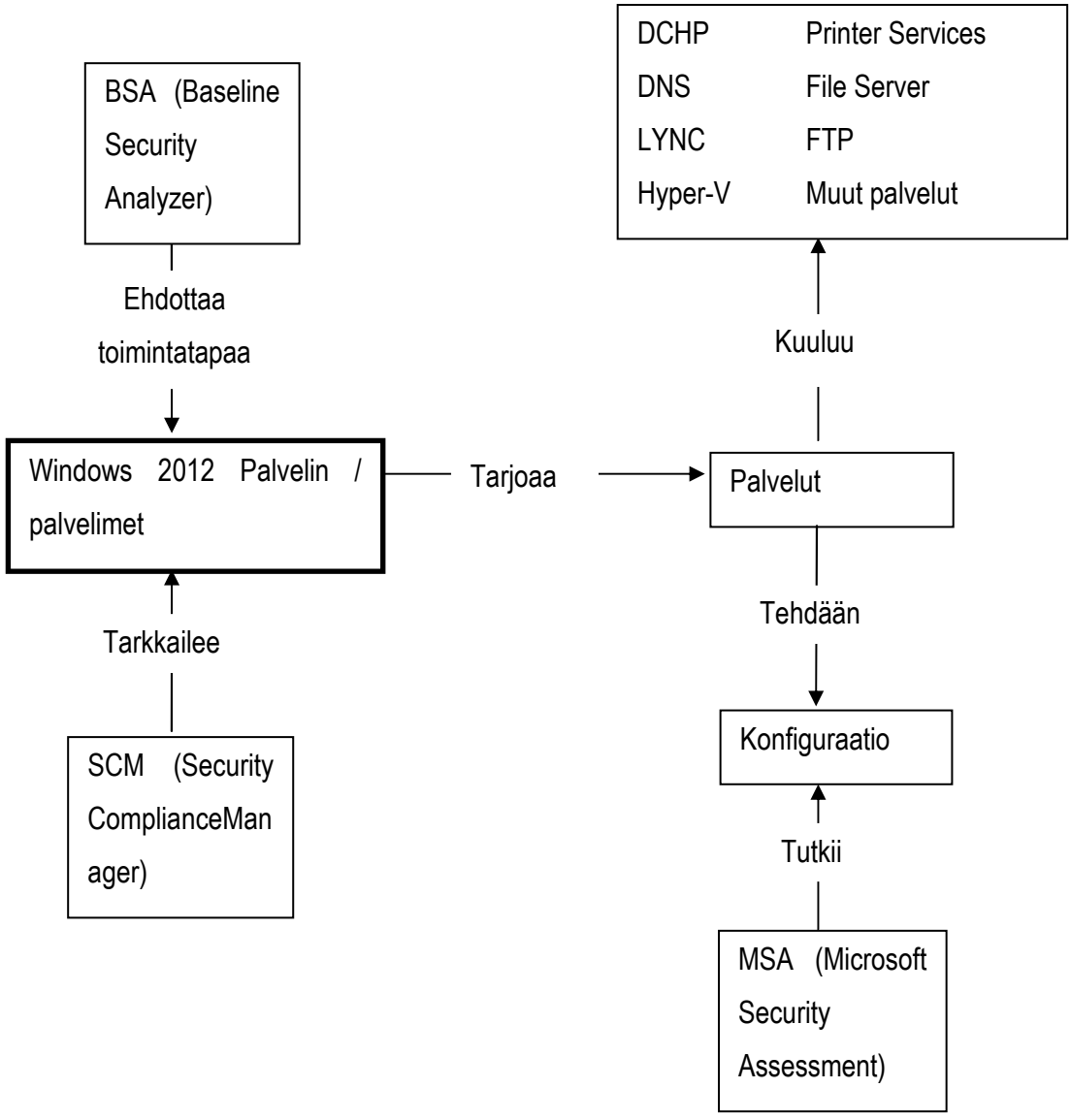
DHCP-palvelun testauksessa Linuxin Ubuntu-jakelulla ajettiin Yersinia-ohjelmistoa. Ohjelmisto oli konfiguroitu lähettämään verkkoon osoitepyyntöjä satunnaisesti generoidulla MAC-osoitteella. Koska paketteja voi lähettää nopeasti kymmeniä tuhansia, on DHCP-palvelu nopeasti palvelunestetyssä tilassa. Yersinia mahdollistaa myös valvomattoman (rogue) DHCP-palvelimen option, jossa väärennettyä informaatiota pystytään jakamaan verkkoon(Ubuntu.com. Hakupäivä 29.5.2014). Koska DHCP-palvelin mahdollistaa myös muun konfiguraation jakamisen, on Yersinia-ohjelmistolla mahdollista väärentää myös nimipalvelutietoa.

Linuxin Kali-jakeluversio on penetraatiotestaukseen tarkoitettu Linux-jakelupaketti. Se on paras yksittäinen alusta järjestelmän penetraatiotestaamiseen. Kali sisältää John The Ripper -ohjelman, mikä pystyy purkamaan salattuja tiedostoja (kuten Windowsin SAM). Kali sisältää myös Wireshark-ohjelmiston pakettien analysointiin. Se on myös tuettu alusta Metasploit-projektin viitekehykselle, joka mahdollistaa tietoturva-aukkojen hyödyntämiseen saatavilla oleviavalmiilla skripteillä ja ohjelmilla (Binarytides 2013. Hakupäivä 29.5.2014).Kali-jakelupakettiin on saatavilla stressitestejä sekä Windows Serverin kaatamiseen, että nimipalvelun tukkimiseen. Tietoturvan perustason ulkopuolelle jäänyt järjestelmä on näille altis. Kali on mahdollista asentaa myös USB-muistille. Tämä mahdollistaa ajamisen suurilla oikeustasoilla ilman paikallista käyttöoikeutta

sekäaiheuttaa myös riskin Windows-alustan paikallisten administrator-oikeuksiensaamiselle. Paikallisten oikeuksien hankkiminen asiakaskoneilta on nopea prosessi, johon on paljon valmiita ohjelmia. Tämän lopputyön yhteydessä niistä käytettiin Cain and Abel-sekä John The Ripper -ohjelmia Kali-käyttöjärjestelmälle sekä Ophcrack-ohjelmaa Windows-alustalle. Kun asiakaskoneelle on saatu hetkessä käytännössä rajattomat oikeudet,on sinne mahdollista asentaa mikä tahansa kuunteleva ohjelma ja ohjata esimerkiksi näppäimistön syötteet yhteen tekstitiedostoon. Järjestelmään pääsyn jälkeen on myös mahdollista asentaa jokin ohjelma (esim. NetCat) avaamaan ohjelmallisia takaovia vaikka koneen käynnistymisen yhteydessä.

6 PERUSTASOON PÄÄSSYT JÄRJESTELMÄ

Perustason saavuttanutta järjestelmää vastasi hyviksi tunnustetuilla tavoilla konfiguroidut palvelut sekä päivitetty Windows 2012 Server -palvelinympäristö. Palvelujen nostaminen Microsoftin määrittelemälle perustasolle tehtiin noudattamalla seuraavaa kaaviota (Kuvio 9).



Kuvio9. Perustason nostamisen käsitekartta.

Windows 2012 -palvelimeen asennettiin DHCP, nimipalvelu ja toimialueohjain. SCM-työkalu tarkkailee palvelimen asetuksien tilaa, johon MBSA antaa ehdotuksen suositelluille

toimintatavoille sekä päivitysten asentamiseksi että konfiguraatioiden suorittamiseksi. MSA-ohjelmistoon syötetty data ympäristön konfiguraation tilasta tutkii, onko hyviä käytänteitä noudatettu. Ohjelmien ajon jälkeen tehdään tarvittavia konfiguraatiomuutoksia ja ajetaan suositellut päivitykset. Tämän jälkeen ohjelmistojen ajo sekä konfiguraatio ja päivitysprosessi toistetaan. Prosessia jatketaan kunnes haluttu tila on saavutettu.

7 RISKIANALYYSI

Riskianalyysi tehtiin vertaamalla testattuja riskejä niiden potentiaaliin vahingoittaa järjestelmää, todennäköisyyteen tapahtua, riskien luomaan vikatilanteeseen sekä kriittisyyteen. Riskianalyysiin valittiin testatuista riskeistä vain osa. Taulukoidut riskit on valittu sillä perusteella, että ne on löydettyMicrosoftin määrittelemään tietoturvan perustasoon pyrkiessä. Riskit nimettiin tehtyjen testien perusteella niiden olennaisimpien uhkien mukaan. Kyvyksi vahingoittaa järjestelmää nimettiin riskin pääasiallinen haitta. Tapahtuman todennäköisyys määriteltiin joko todennäköiseksi, mahdolliseksi tai epätodennäköiseksi. Vikatilanteeksi määriteltiin onnistuneen hyökkäyksen aiheuttama haitta. Kriittisyyden asteikoksi määriteltiin heikko, keskitaso tai vakava.

On huomattava, että riskianalyysissä mukana olleita riskejä ei voi poistaa vain pyrkimällä Microsoftin määrittelemään tietoturvan perustasoon. Ne on kuitenkin *havaittavissa* esitellyillä Microsoftin työkaluilla joko suoraan tai seuraamalla verkon liikennettä muilla niihin tarkoituksiin saatavilla olevilla ohjelmistoilla.

Testattujen riskien perusteella voidaan sanoa, että DHCP-palvelinta koskevat riskit ovat todennäköisimpiä. Niiden kriittisyys oli heikkoa tai keskitasoa. Poikkeuksena oli DHCP - ja nimipalvelimen yhteinen asentaminen valvomattomaksi (rogue) palvelimeksi. Todennäköisin DHCP-palvelua koskeva riski oli verkko-osoitteiden kuluttaminen poolista. Tämä johtui riskin toteuttamisen helppoudesta.

Nimipalvelimen kyselytulva määriteltiin todennäköisyydeltään mahdolliseksi ja sen kriittisyys oli vakava. Tämä johtui useista nimipalvelimen toimintaa koskevista vikatilanteista. Nimipalvelua koskeva kyselytulvan riski oli kuitenkin epätodennäköinen.

Toimialueohjaimen hash-salasanojen vuoto ja hash-autentikointi luokiteltiin vakavaksi kriittisyydeltään. Tämä johtui toimialueohjaimen keskeisestä toiminnasta koko verkolle. Toimialueohjaimen vikatilanteita olivat pääsy verkkoresursseihin.

Kakkia riskejä ei ole raportoitu.

Taulukko1. Riskianalyysi

Riski	**Kyky vahingoittaa järjestelmää**	**Tapahtuman todennäköisyys**	**Vikatilanne**	**Kriittisyys**
DHCP: Poolin osoitteiden kuluttaminen loppuun	Osoitteiden loppuminen poolista	Todennäköinen	DoS	Heikko
DHCP: Auktorisoimattomat asiakkaat	Tiedostojen kopiointi	Todennäköinen	Pääsy verkkoresursseihin	Keskitaso
DHCP / Nimipalvelin: Valvomaton palvelin	Verkon kuormittaminen, asiakaskoneiden saastuttaminen	Mahdollinen	DNS välimuistin myrkytys, asiakaskoneiden DoS, uudelleenohjaus	Vakava
Nimipalvelin: kyselytulva	Verkon ja nimipalvelimen kuormittaminen	Epätodennäköinen	DoS	Heikko
Toimialueohjain: Hash-salasanat	Salasanojen vuotaminen	Mahdollinen	Pääsy verkkoresursseihin	Vakava
Toimialueohjain: Hash-autentikointi	Auktorisoimaton hallinta	Epätodennäköinen	Pääsy verkkoresursseihin	Vakava

8 TULOKSET

Testien tulokset käytiin kokonaisuudessaan läpi palaverissa 20.5.2014 Oulun ammattikorkeakoulun it-palvelussa. Tulokset mahdollistavat järjestelmän tietoturvan tason nostaminen Microsoftin perustason yläpuolelle sekä auttavat sulkemaan tietoturva-aukkoja.Lopputyölle määritellyt tavoitteet saavutettiin.

Testeistä saatujen tulosten perusteella voidaan sanoa, että pelkkä Microsoftin määrittelmän perustason saavuttaminen ei riitä turvaamaan koko järjestelmää. Se ei poista kaikkia tietoturvariskejä eikä sitä voi jättää ainoaksi tietoturvakeinoksi. Riskejä paljastuu niin paljon koko ajan, ettei pelkän perustason varaan voi rakentaa ison organisaation tietoturvaa.

Microsoftin perustason saavuttamista on silti syytä tavoitella. Se on hyvä lähtökohta järjestelmän tietoturvan kehittämiseen. Määrittely on perusteellisesti tehty ja siihen liittyy paljon hyviksi todettuja ja testattuja käytäntöjä. Perustasoon päästä helpottavat valmiit ohjelmistot ja dokumentaatio. Sekä ohjelmat, että niihin kuuluva dokumentointi ovat maksuttomia.

Kun organisaation tietoturvatasoa nostetaan eli järjestelmää kovetetaan, laskee samalla käytettävyyden taso. Tämän takia tietoturvaa ei voi nostaa pääprioriteetiksi. Käytössä olevia järjestelmiä, ohjelmistoja ja laitteita on pystyttävä käyttämään tietoturvan nostamisesta huolimatta. Microsoftin määrittelemän perustason valttina on tasapainotettu tila, missä tietoturvan taso on korkealla ja helposti edelleen kovetettavissa mutta järjestelmä edelleen käyttäjäystävällinen.

9 JOHTOPÄÄTÖKSET

Microsoftin määrittelemän perustason saavuttaminen ei poista kaikkia tunnettuja riskejä testatuissa palveluissa. Testatut riskit hyväksikäyttävät palveluiden toimintaa siten, miten niiden on tarkoituskin toimia. Näin ollen perustason määrittäminen ei vaikuta niiden kykyyn haitata järjestelmää.

Tämä ei kuitenkaan tarkoita sitä, että Microsoftin määrittelemään perustasoon pyrkiminen ei olisi suositeltavaa. Microsoftin tietoturvatasoa tarkkailevien ja suositeltuja konfiguraatio-ohjeita antavien ohjelmistojen avulla järjestelmää voidaan helposti kovettaa, ja sen tietoturva-aukoista on helpompi olla tietoinen. Perustasoon pyrkiminen nostaa tietoturvan tasoa sekä helpottaa järjestelmää koskevien tietoturvapäivitysten seuraamista.

Microsoftin työkalut tietoturvan perustasoon pyrkimiseen ovat hyviä. Ne ovat toiminnoiltaan monipuolisia ja niitä on helppo käyttää. Microsoftin dokumentointi näiden ohjelmistojen osalta on kiitettävä. Eniten hyötyä perustasoon pyrkimisen kannalta oli MSA:lla ja MBSA:lla. Niiden ohjeet olivat helppoja seurata ja asennus toimi kuten pitikin. SCM osoittautui työkaluista selvästi huonoimmaksi, ja pelkkä asentaminenkin Windows Server 2012 ympäristöön oli ongelmallista. SCM ei ole toimintavarma Windows 2012 -ympäristössä. Se sisältää tunnettuja vikoja kyseisellä alustalla.

Järjestelmän tietoturvan tila ei ole staattinen kokonaisuus. Järjestelmän jatkuva laajeneminen tuo ongelmia tietoturvan hallitsemisen kannalta. Tunnettujen tietoturvauhkien tunnistaminen ja ehkäiseminen pelkkiä päivityspaketteja asentamalla ei riitä. Järjestelmän laajetessa myös sen sisältämät riskit lisääntyvät palveluiden ja ohjelmistojen määrän kasvaessa. Perustason määrittäminen on helppo tapa nostaa järjestelmän tietoturvan tasoa ja seurata sen muuttuvaa tilannetta.

10 POHDINTA

Olin työharjoittelussa Oamk:nit-palveluissa lähituessa syksyn 2013. Tuona aikana pohdin lopputyön aihetta tietoturvasta. Työharjoittelun loppupuolella sain mahdollisuuden tehdä lopputyön liittyen tietoturvan perustason määrittämiseenMicrosoft:n käytänteiden mukaan. Pääsin jatkamaan luontevasti työskentelyä jo tuttujen it-ammattilaisten kanssa. Vaikka suurin osa itse työstä suoritettiin virtuaalialustalla, oli tilaajan puolelta vastuussa olevasta yhteyshenkilöstä paljon apua.

Opinnäytetyöni alkoi lokakuussa 2013 ja päättyi kesäkuun 2014 alussa. Pitkittynyt aikataulu johtui muista opinnoista. Opinnäytetyöni eteneminen sujui suunnitellusti poislukien aihealueen rajaaminen palveluiden määrittelyyn liittyen opinnäytetyöni alussa.

Itse aiheesta ei löytynyt juurikaan kirjallista materiaalia. Suurin osa perustasoon liittyvistä taustatiedoista tuli Technet-portaalista ja yksittäisten asiantuntijoiden verkkosivuille keräämistä artikkeleista. Palveluiden perustoimintojen lähteiksi löytyi hyvin kirjallista materiaalia kirjastosta.

Opinnäytetyön tarkoituksena oli selvittää, nostaako Microsoftin määrittelemän tietoturvan tason saavuttaminen olennaisesti koko järjestelmän tietoturvaa. Vaikka palveluista testattiin vain kolmea, testaamisen laajuus yllätti. Tunnettujen riskien löytäminen oli yllättävän helppoa ja lähteitä potentiaalisten riskien löytämiseen paljon.

Stressitestattavien palveluiden riskien käytännön toteuttaminen oli aluksi vaikeaa. Lähes kaikki stressitesteihin liittyvät ohjelmistot olivat jollain Linux-jakelulla ajettavia ja niihin tutustumiseen meni käytännön toteutuksessa eniten aikaa. Varsinkin metasploit-alusta oli uusi kokemus siihen saatavineen ohjelmineen. Kaikki riskit ja niiden toteuttamiseen tarkoitetut työvälineet ja menetelmät oli kuitenkin niin hyvin dokumentointu, että hyvillä perustiedoilla toteutus oli mahdollinen.

Opinnäytetyön tekeminen oikealle tilaajalle lisäsi motivaatiota opiskella tietoturva-aukoista laajasti myös työn ulkopuolella. Opituistatiedoista oli merkittävää hyöty työn tekemiseen ja lopputulosten

saamiseen. Myös tilaajalta saatu tuki ja yhteistyö palvelujen määrittämiseen, opinnäytetyön rajaamiseen ja tietoturva-aukkojen tutkimiseen oli hyvä.

Tulevan työelämän kannalta asiantuntijatehtävissä toimiminen vaatii tietoturva-asioiden syvällistä ymmärrystä. Opinnäytetyö antoi valmiuksia oppia enemmän suurten organisaatioiden tietoturvasta ja sen nykytilanteesta sekä kehittämisestä jatkossa.

11 LÄHTEET

Anttila, A. TCP/IP-tekniikka. 2001. Helsinki: Helsinki Media 2000. 202-218,232

Bashar Ewaida. SANS Institute. 2010. Pass-the-hash attacks: Tools and Mitigation. http://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283?show=pass-the-hash-attacks-tools-mitigation-33283&cat=testing

Binarytides 2013.Reviewing Kali Linux – the distro for security geeks.Hakupäivä 29.5.2014. http://www.binarytides.com/kali-linux-security-distro/

Cisco. 2008. Network Security Baseline. Hakupäivä 21.5.2014. http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook.html

CVE Details. 2013. Vulnerability Details : CVE-2013-3868. Hakupäivä 6.5.2014http://www.cvedetails.com/cve/CVE-2013-3868/

CVE Details. 2013. Vulnerability Details : CVE-2013-3869. Hakupäivä 6.5.2014http://www.cvedetails.com/cve/CVE-2013-3869/

IETF tools. The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4. Hakupäivä 29.5.2014.http://tools.ietf.org/html/rfc3442

IETF tools.Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4).Hakupäivä 29.5.2014.http://tools.ietf.org/html/rfc3396

Information Security Standards. 2008. ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition). Hakupäivä 21.5.2014.http://www.iso27001security.com/html/27005.html

Kivimäki, J. Windows Server 2008R2 Tehokas hallinta. 2009. Helsinki: Readme.fi. ,473, 478, 479, 601.

Kuvio1. Waarith.com. 2013. Hakupäivä 29.5.2014.http://www.waarith.com/information__management_technology/network_infrastructure

Kuvio2. DCHP-palvelimen toiminta. certshelp. 2012. Hakupäivä 9.3.2014http://www.certshelp.com/blog/how-dhcp-servers-works/

Kuvio3. DNS-palvelimen toiminta. Spiceworks. 2009. Hakupäivä 29.5.2014http://community.spiceworks.com/how_to/show/480-how-dns-works

Kuvio4. Toimialueohjain verkossa. Scientificera. 2012. Hakupäivä 29.5.2014.http://scientificera.com/windows/45-windows/224-what-is-a-domain-controller.html

Laaksonen, M. Nevasalo, T. Tomula, K. Yrityksen tietoturvakäsikirja. 2006. Helsinki: Edita publishing Oy 2006. 155

Microsoft Technet. 2013.Windows Server 2012 Security Baseline. Hakupäivä 9.12.2013.http://technet.microsoft.com/en-us/library/jj898542.aspx

Microsoft Technet. 2003. What is DHCP? Hakupäivä 18.12.2013.http://technet.microsoft.com/en-us/library/cc781008(v=ws.10).aspx

Microsoft. 2009. Microsoft Security Assessment Tool 4.0. Hakupäivä 6.5.2014.http://www.microsoft.com/en-us/download/details.aspx?id=12273

Microsoft. 2014. Microsoft Security Assessment Tool 4.0. Hakupäivä 6.5.2014.http://www.microsoft.com/en-us/download/details.aspx?id=12273

Microsoft Tehcnet. Security Compliance Manager (SCM). Hakupäivä 6.5.2014.http://technet.microsoft.com/fi-fi/solutionaccelerators/cc835245.aspx

Noarthcutt S, Novak J.2002. Verkkomurtojen havaitseminen - Analyytikon käsikirja. Suom. Pekka Saxberg. Helsinki: Satku. Alkuperäisjulkaisu 2001.

Pitkänen, J. Tietokone, 2008. Microsoft Baseline Security Analyzer. Hakupäivä 10.1.2014.http://www.tietokone.fi/artikkeli/arkisto/windows/microsoft_baseline_security_analyzer

SANS-institute 2000-2002.Global Information Assurance Certification Paper.Hakupäivä 29.5.2014. http://www.giac.org/paper/gcwn/15/disable-nonessential-devices-services-reduce-exposure-dos-attacks/100301

Securelist. What is phishing? Hakupäivä 28.4.2014. https://www.securelist.com/en/threats/spam?chapter=85

The TCP/IP guide. 2005. DHCP Security Issues. Hakupäivä 18.12.2013. http://www.tcpipguide.com/free/t_DHCPSecurityIssues.htm

TCP/IP guide. 2005. Using Multiple DNS Servers to Spread Out DNS Requests. Hakupäivä 29.5.2014. http://www.tcpipguide.com/free/t_DNSNameServerLoadBalancing.htm

Ubuntu.com. Yersinia - A FrameWork for layer 2 attacks. Hakupäivä 29.5.2014http://manpages.ubuntu.com/manpages/hardy/man8/yersinia.8.html

WindowsSecurity.com. 2011. DNS Security part1: Issues in DNS security. Hakupäivä 28.4.2014http://www.windowsecurity.com/articles-tutorials/misc_network_security/DNS-Security-Part-1.html