TAMPEREEN
AMMATTIKORKEAKOULU

KEHITTYNEET KYBERUHAT JA NIIDEN VALVONTA

Microsoft Advanced Threat Analytics

Sami Lylyoja

Opinnäytetyö
Toukokuu 2017
Tietojenkäsittely
Tietoverkkopalvelut

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Tietoverkkopalvelut

LYLYOJA, SAMI:
Kehittyneet kyberuhat ja niiden valvonta
Microsoft Advanced Threat Analytics

Opinnäytetyö 63 sivua
Toukokuu 2017

Opinnäytetyö toteutettiin Tampereen ammattikorkeakoulun tietojenkäsittelykoulutuksen WPK-verkolle, joka on tietojenkäsittelyn opiskelijoiden ja opettajien ylläpitämä ja kehittämä harjoitus- ja laboratorioverkko. Kirjoittaja suoritti harjoittelunsa verkon ylläpitäjänä ja idea opinnäytetyöstä syntyi harjoittelun aikana, kirjoittajan oman mielenkiinnon pohjalta.

Opinnäytetyön tavoitteena oli tutkia, onko verkko altis kehittyneiden kyberhyökkäysten uhille tai onko siinä heikkouksia jotka mahdollistavat kirjautumistunnusten väärinkäytön. Työn tarkoituksena oli asentaa Microsoftin Advanced Threat Analytics -ohjelmisto verkkoa valvomaan ja tarkastella kolmen kuukauden seurantajakson aikana ohjelman havaitsemia uhkia ja heikkouksia.

Työssä tutkittiin Windowsin todennusprotokollia, kyberhyökkäysketjujen vaiheita ja erilaisia kehittyneitä hyökkäysmenetelmiä, joita voidaan toteuttaa Mimikatz-ohjelman ja etätyökalujen avulla. Työ selvittää vaiheittain ja esimerkkien avulla, miten moderni kyberhyökkäys voi edetä kohdeverkossa yhdeltä laitteelta aina verkon toimialuepalvelimelle asti. Lisäksi se esittelee Microsoftin tarjoaman käyttäjien ja kohteiden valvontaohjelmiston, jonka avulla kyberhyökkäyksiä voidaan havaita.

Opinnäytetyön toteutuksen aikana WPK-verkossa havaittiin muutamia heikkouksia, joiden vuoksi hyökkääjän tai opiskelijan olisi helppo varastaa toisen käyttäjän kirjautumistietoja. Varastettujen kirjautumistietojen avulla hyökkääjän tai opiskelijan olisi mahdollista päästä käsiksi resursseihin, joihin hänellä ei ole oikeutta, tai pahimmassa tapauksessa lamauttaa koko verkon toiminta. Työn tuloksena verkossa saatiin korvattua osassa laitteista käytössä ollut heikko todennusprotokolla ja lisäksi havaittiin verkkoon tehty tiedusteluhyökkäysharjoitus.

Nykyään mikään tietoturvaratkaisu ei pysty tarjoamaan täydellistä suojaa kyberhyökkäyksiltä. Hyökkääjä voi olla myös sisäpiiriläinen, jolloin käyttäjien ja kohteiden käyttäytymisanalyysiin perustuva valvontasovellus on tehokas tapa havaita hyökkäykset ja käyttäjien poikkeava toiminta verkossa. Tärkeimpänä kehitysehdotuksena kirjoittaja suosittaa WPK-verkon Windows 7 -laitteiden päivittämistä uudempiin käyttöjärjestelmiin mahdollisimman nopeasti, koska uudemmat käyttöjärjestelmät ovat huomattavasti paremmin suojattuja erityisesti kirjautumistietojen varastamishyökkäyksiä vastaan.

Asiasanat: kyberuhat, hyökkäysketjut, valvonta, ata, mimikatz

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Network Services

LYLYOJA, SAMI:
Advanced Cyber-Threats and Monitoring
Microsoft Advanced Threat Analytics

Bachelor's thesis 63 pages
May 2017

This bachelor’s thesis was commissioned by the WPK laboratory network at Tampere University of Applied Sciences. The initial idea for this thesis was born from the author's interest in cyber-attacks when he was performing his internship as the network’s administrator trainee.

The objective of this thesis was to find out if the WPK network is vulnerable to different kinds of cyber-threats and credential theft techniques, which allow the misuse of other people’s login credentials. The purpose of this thesis was to install Microsoft’s Advanced Threat Analytics to monitor the network and gather behavioral data from its users. The work included a three-month follow-up time during which data from the monitoring software was reviewed and development suggestions were made based on the findings.

An overview of Windows authentication protocols and different stages of cyber-attack kill chain is offered in this thesis. The reader is presented with concrete how-to examples of different kinds of login credential theft and lateral movement techniques with the use of the Mimikatz tool in an Active Directory network environment.

As a result of this study, vulnerabilities and weak authentication protocols were found to exist in the WPK network. During follow-up time, the monitoring software also detected an unreported practice reconnaissance attack, which took place in the network.

No security solution can guarantee 100% protection from advanced cyber-attacks. The attacker can also be an insider, in which case software that is based on user and entity behavior analysis offers an effective way to detect abnormal behavior. It is recommended that computers with Windows 7 should be upgraded without delay to a newer operating system, which offers much better protection against credential theft techniques.

Key words: cyber-threats, kill-chains, monitoring, ata, mimikatz

SISÄLLYS

LYHENTEET JA TERMIT

AES	Advanced Encryption Standard, lohkosalausmenetelmä.
AS	Authentication Service, todennuspalvelu jota käytetään Kerberos-protokollassa.
DES	Data Encryption Standard, heikko lohkosalausmenetelmä.
HMAC	Hashed Message Authentication Code, tietoliikenteen eheyden tarkistuksessa käytetty standardi.
KERBEROS	Windowsissa käytössä oleva todennusprotokolla.
KDC	Key Distribution Center, avaintenjakelukeskus, palvelin jota käytetään Kerberos-protokollassa luotettuna tahona.
LM-TIIVISTE	LAN Manager / Local Area Network Manager, Windowsissa käytetty vanha salasanan tiiviste.
LSASS	Local Security Authority Subsystem Service, Windowsin palvelu jonka vastuulla todentaminen on.
MD	Message Digest, hajautusalgoritmi.
NTLM	New Technology Local Area Network Manager, Windowsissa käytössä oleva todennusprotokollapino.
NT-TIIVISTE	New Technology, NTLM-protokollassa käytetty uudempi salasanan tiiviste.
SAM	Security Account Manager, paikallisten käyttäjätietojen tallennuspaikka.
SID	Security Identifier, käyttäjien ja ryhmien tunnistekoodi.
SPAN	Switched Port Analyzer, portin peilaus menetelmä.
SSO	Single-Sign-On, kertakirjautuminen.
TGS	Ticket Granting Service, lipun myöntävä palvelu Kerberos-protokollassa.
TGT	Ticket Granting Ticket, lipun myöntävä lippu jota käytetään Kerberos-protokollassa.
RID	Relative Identifier, SID-tunnisteen viimeiset merkit.

1 JOHDANTO

New York Times kirjoitti jo vuonna 2013, että tietoturva-asiantuntijoiden mukaan ei ole kuin kahdenlaisia yrityksiä, sellaisia jotka ovat jo hakkeroitu ja sellaisia jotka eivät tiedä olevansa hakkeroituja (Perlroth 2013). Tänä päivänä on yleisesti hyväksytty ns. oletetun tunkeutumisen ajatusmalli, jossa lähtökohta on, että mikään ei voi tarjota sataprosenttista suojaa kyberhyökkäyksiltä vaan tarpeeksi päättäväinen ja taitava hyökkääjä löytää aina tien sisään järjestelmään. Mitä vaiheita ja tekniikoita tällainen hyökkäys pitää sisällään? Onko niitä mahdollista havainnoida? Muun muassa näihin kysymyksiin tämä opinnäytetyö pyrkii vastaamaan.

Opinnäytetyössä käydään lävitse Microsoft Windows -käyttöjärjestelmän käyttämät todennusprotokollat NTLM ja Kerberos ja selvitetään miten modernin kyberhyökkäyksen vaiheet etenevät tiedustelusta poistumiseen tai verkon haltuunottoon. Opinnäytetyö sisältää käytännön esimerkkejä miten erilaisia kyberhyökkäystekniikoita voidaan toteuttaa Active Directory -ympäristöissä. Lisäksi opinnäytetyössä esitellään Microsoftin Advanced Threat Analytics -ohjelmisto, joka on kehittyneiden kyberuhkien havainnointiin tarkoitettu UEBA-ratkaisu (User and Entity Behavioral Analytics). Ohjelmiston asennuksen vaiheet käydään pääpiirteittäin lävitse, mutta varsinaiseksi ohjelmiston asennusohjeeksi opinnäytetyöstä ei ole.

Opinnäytetyö sai alkunsa kirjoittajan kiinnostuksesta aihepiirin ja se toteutuksen toimeksiantajana ja mahdollistajana toimi Tampereen ammattikorkeakoulun tietojenkäsittelyn koulutus, jonka harjoitus- ja laboratorioverkko WPK:n ylläpitäjänä kirjoittaja suoritti harjoittelunsa. Opinnäytetyön tavoitteena oli tutkia, onko ammattikorkeakoulun WPK-verkossa heikkouksia tai onko se muuten altis kehittyneiden kyberhyökkäysten uhille, joita hyväksikäyttämällä hyökkääjä tai opiskelija voisi ottaa verkon hallintaansa tai aiheuttaa muuta vahinkoa verkolle tai sen käyttäjille.

Opinnäytetyön tarkoituksena oli asentaa Microsoftin Advanced Threat Analytics -ohjelmisto WPK-verkkoa valvomaan ja seurata kolmen kuukauden ajan ohjelman havaintoja verkossa. Samalla tarkoituksena oli tarjota tuleville ylläpitäjille helppokäyttöinen työkalu, jonka avulla verkkoa voidaan valvoa erilaisten kyberuhkien varalta.

2 PÄÄSYNHALLINTA

2.1 Todennus

Todennuksen eli autentikaation tarkoitus on varmistaa, että käyttäjät tai objektit ovat keitä he väittävät olevansa. Käyttäjän todennuksessa yhdistetään yleensä kirjautumistunnus ja salasana, joilla saadaan luotua identiteetti käyttäjälle. Objektien kohdalla pyritään varmistamaan identiteetin sijaan objektin aitous. (TechNet 2013.) Käyttäjälle näin luotua identiteettiä voidaan käyttää myös käyttöoikeuksien myöntämiseen ja kieltämiseen, sekä käyttäjien ja palveluiden valvontaan.

Todennusta ei ole kuitenkaan välttämätöntä suorittaa käyttäjänimellä ja salasanalla, eli tiedolla joka aidolla käyttäjällä on. Siihen voidaan käyttää myös erilaisia elektronisia turvamerkkejä, biometrisiä tunnisteita tai sertifikaatteja, eli jotain mitä aidolla käyttäjällä on. Myös näiden kahden todennuksen erilaiset yhdistelmät ovat mahdollisia, jolloin kyseessä on ns. kaksivaiheinen todennus. (TechNet 2013.)

Käyttäjän todennus suoritetaan todennusprotokollan avulla, joita Microsoft Windows -käyttöjärjestelmissä on tuettuna useita. Näihin kuuluvat esim. uudempi Kerberos-protokolla, jota käytetään AD-toimialue todennuksessa ja vanhempi NTLM-protokolla, jota käytetään mm. työryhmälaitteiden todennusprotokollana.

2.1.1 NTLM-protokolla

NTLM on Windows-käyttöjärjestelmiin sisäänrakennettu turvallisuusprotokollapino, jonka tarkoituksena on mahdollistaa käyttäjien todennus, sekä taata datan eheys ja luottamuksellisuus. NTLM-protokollapino sisältää vanhemman LAN Managerin versiot 1 ja 2, sekä uudemman NTLM:n versiot 1 ja 2. (TechNet 2012.)

NTLM:n ensimmäinen versio julkaistiin jo vuonna 1993, aiemmin käytetyn Windowsin salasanavarasto Microsoft LAN Managerin seuraajaksi. Siinä missä ns. LANMAN käytti todennukseen LM-tiivistettä, siirryttiin NTLM:ssä käyttämään uutta NT-tiivistettä, joka oli huomattavasti turvallisempi kuin edeltäjänsä. Vanha LM-tiiviste ei mm. erotellut

lainkaan salasanojen isoja ja pieniä kirjaimia, vaan kaikki salasanojen merkit muutettiin isoiksi kirjaimiksi ennen tiivisteen luontia. Lisäksi suurin sallittu salasanan pituus oli 14 merkkiä ja yli seitsemän merkkiset salasanat jaettiin kahteen osaan tiivistettä luodessa. (Johansson 2006; Jungles ym. 2012, 35.)

Vaikka LM-tiiviste on vanhentunut ja sen tietoturva on todella heikko, saattaa siihen vieläkin törmätä mm. kolmansien osapuolien SMB-ratkaisuissa ja vanhoissa käyttöjärjestelmissä. LM-tiiviste luodaan DES-algoritmin avulla, joka on nykyisin helposti murrettavissa. Tämä tarkoittaa, että LM-tiiviste on mahdollista muuttaa takaisin selkotekstiseksi salasanaksi. Tiivisteen paljastuminen onkin siksi suoraan verrannollinen salasanan paljastumiseen. LM-tiivisteen turvattomuuden vuoksi se on ollut Windows-käyttöjärjestelmissä oletuksena pois päältä jo Windows Vistasta lähtien, eikä Microsoft suosittele enää sen käyttämistä. (Barret, Weiss & Hausman 2015.)

NTLM:ssä esitelty uudempi NT-tiiviste on turvallisempi, koska se tukee suurempia määriä merkkejä (142 vs. 65 536) ja erottelee isot ja pienet kirjaimet. Lisäksi NT-tiivisteen luomiseen käytetään kokonaista salasanaa, jonka suurin sallittu pituus on 127 merkkiä 14 merkin sijaan. NT-tiivisteen luomiseen käytetään myös turvallisempaa MD4-algortimia vanhemman DES-algoritmin sijaan. (Wu & Irwin 2013, 897-898.)

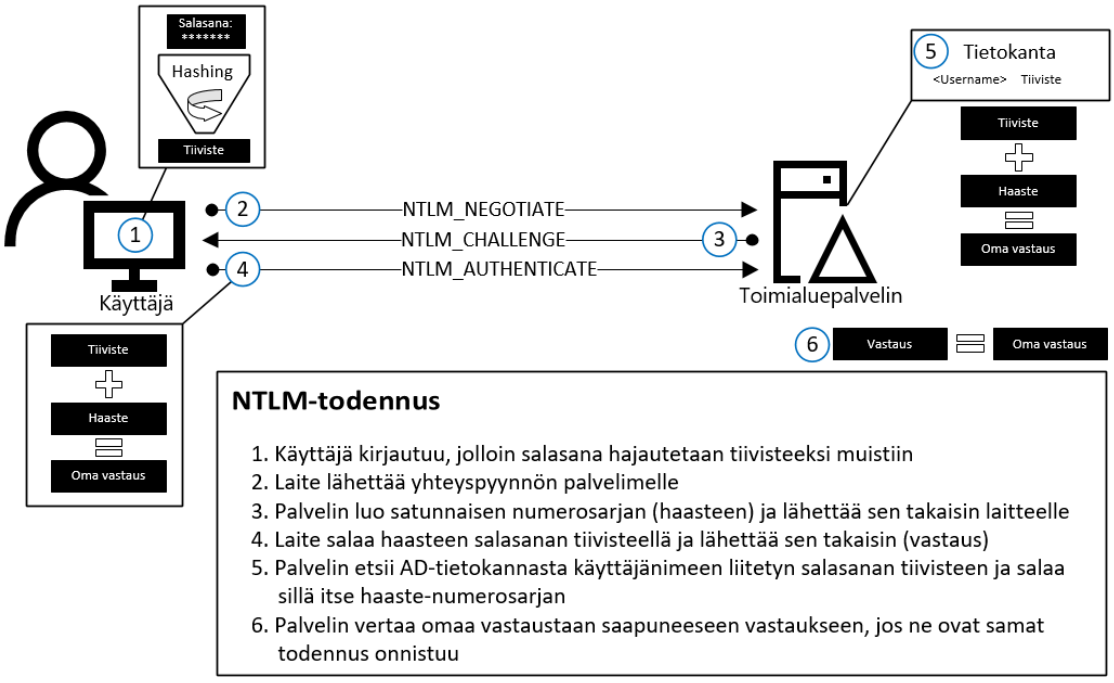
NTLM-protokolla päivitettiin vuonna 1998 versioon kaksi, joka paransi sen turvallisuutta edelleen ottamalla haaste-vaste -menetelmässä käyttöön HMAC-MD5-algoritmin. Lisäksi se mahdollisti protokollassa molemminpuolisen todentamisen. (Barret ym. 2015.) Vaikka NTLM-protokollapinossa on edelleen olemassa tuki molemmille, LM- ja NT-tiivisteille, tarkoitetaan termiä NTLM-tiiviste käytettäessä yleensä nykyisin ainoastaan uudempaa NT-tiivistettä. (Wu & Irwin 2013, 897.) Taulukossa 1 on vertailtu eroja näiden eri salasanan tiivisteiden välillä.

TAULUKKO 1. Windowsin salasanojen tiivisteet (EC-Council 2010, 5-12)

	LM:	NTLMv1:	NTLMv2:
Kirjasinkoko	Ei	Kyllä	Kyllä
Hajautus-algoritmi	DES (ECB)	MD4	MD4
Tiivisteen pituus	64-bit+64-bit	128-bit	128-bit
H-V -avaimen pituus	56-bit+56-bit+16bit	56-bit+56-bit+16bit	128-bit
H-V -algoritmi	DES (ECB)	DES (ECB)	HMAC-MD5

Tänä päivänä NTLM-protokolla on syrjäytetty toimialueympäristöissä Kerberos-protokollan toimesta. NTLM on kuitenkin edelleen oletustodennusprotokolla itsenäisissä Windows-ympäristöissä, jotka eivät ole toimialueen jäseniä. Lisäksi sitä käytetään Windows NT -käyttöjärjestelmissä ja tilanteissa, joissa todennutaan palvelimelle käyttäen IP-osoitetta. (Regan 2014, 384.)

NTLM-todennus tapahtuu käyttämällä haaste-vaste -menetelmää, jossa asiakas todennetaan ilman, että salasanaa lähetetään verkon yli. Tämä tapahtuu siten, että asiakas suorittaa laskutoimituksen jonka vastaus osoittaa, että asiakkaalla on tiedossa käyttäjänimeen liitetty salasana. (Regan 2014, 384.) NTLM-todennuksen vaiheet on esitelty kuviossa 1.



KUVIO 1. NTLM-todennuksen toimintaperiaate toimialueella (Microsoft 2016b, n.d.)

NTLM-protokollan etuihin uudempaan Kerberos-protokollaan verrattuna voidaan laskea ainoastaan sen helppokäyttöisyys ja täysi yhteensopivuus vanhempien Windows-käyttöjärjestelmien kanssa. NTLM:n heikkoudet puolestaan ovat sen haavoittuvuus kirjautumistietojen varastamishyökkäyksille ja vanhentuneiden salaustekniikoiden käyttö, jotka mahdollistavat salasanojen tiivisteiden murtamisen. (Wu & Irwin 2013, 898.) NTLM ei myöskään tue lainkaan uudempia salaustekniikoita kuten AES (Advanced Encryption Standard), jonka vuoksi Microsoft ei suosittele enää NTLM-todennuksen käyttöä, vaan kehottaa kehittäjiä siirtymään Kerberos-protokollaan (Microsoft 2016b).

2.1.2 Kerberos-protokolla

Kerberos on TCP/IP-verkkoihin suunniteltu todennusprotokolla, jonka kehitys aloitettiin Massachusetts Institute of Technology yliopistossa Project Athene nimellä jo 1980-luvun alussa. Kerberos pohjautuu Needham-Schroeder -avaintenjakoprotokollaan ja se on osa TCP/IP-protokollapinon ns. vapaita protokollia. Tästä johtuen se on yhteensopiva useiden laitteiden kanssa, valmistajasta ja käyttöjärjestelmästä riippumatta. (Schneier 2015.)

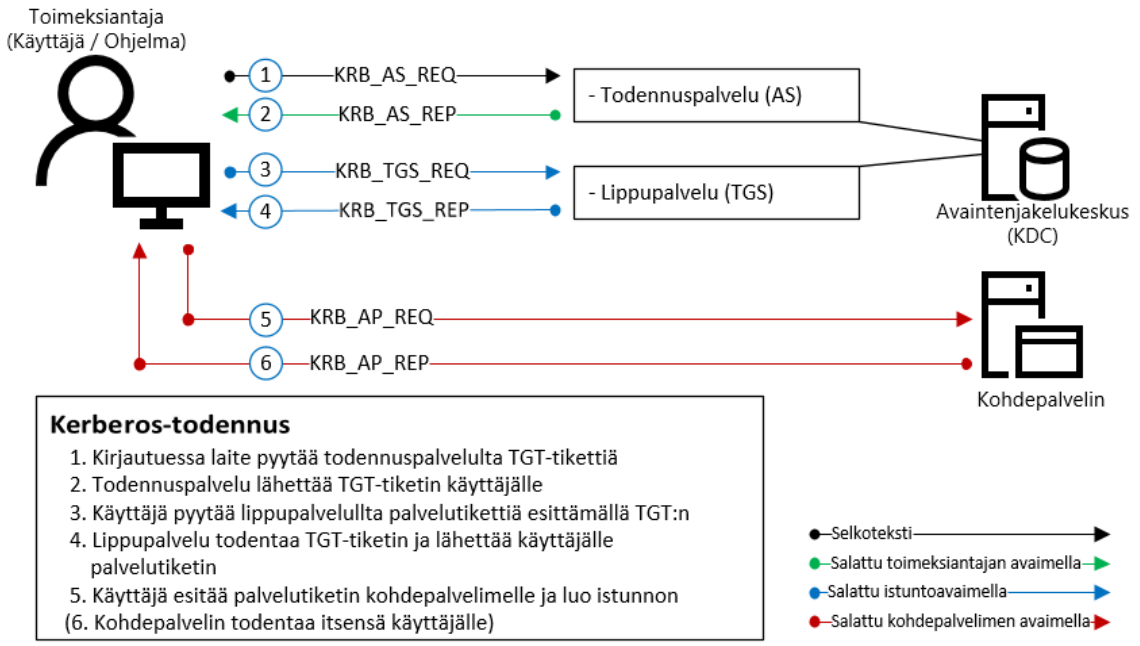
Tänä päivänä käytössä oleva Kerberoksen 5. versio on oletustodennusprotokolla kaikissa Windows AD-toimialuelaitteissa ja lisäksi sitä käytetään mm. Linuxin ja Applen -käyttöjärjestelmissä. Protokolla mahdollistaa toimeksiantajan (käyttäjä/palvelin/palvelu) identiteetin varmentamisen turvallisella tavalla suojaamattomien verkkojen yli. Kerberos mahdollistaa lisäksi molemminpuolisen todennuksen, eli toimeksiantajan lisäksi myös palvelin voidaan määrittää todentamaan itsensä. (Abernathy & McMillian 2016.)

Kerberos käyttää todentamisessa apuna symmetristä salausta eli ns. salaisen avaimen menetelmää, jossa molempien osapuolien on tiedettävä avain, jolla viesti salataan ja puretaan. Kerberoksessa jokaiselle kohteella on kuitenkin oma erillinen avaimensa. Alun perin Kerberoksen 5. versiossa oli käytössä DES-salausalgoritmi, mutta uudemmat Windows-käyttöjärjestelmät mahdollistavat myös turvallisemman AES-salausalgoritmin käytön (Wu & Irwin 2013, 1118).

Kerberos-protokolla koostuu kolmesta osasta jotka ovat asiakas, palvelin ja luotettu kolmas osapuoli. Luotetusta kolmannesta osapuolesta käytetään nimitystä Key Distribution Center, eli avaintenjakelukeskus. Tämä ns. KDC-palvelin on protokollassa luotettu taho, koska palvelin tietää kaikkien verkon käyttäjien, laitteiden ja palveluiden tunnukset ja salasanat. Asiakas on toimeksiantaja, eli taho joka haluaa saada pääsyn verkossa olevaan palveluun tai resurssiin. Asiakkaana voi olla käyttäjä, ohjelma tai palvelu. Palvelin puolestaan on päätepiste, jolla käytettävä ohjelma tai resurssi sijaitsee. (Gordon 2015, 665-666.)

KDC-palvelimella pyörii kaksi erillistä palvelua, todennuspalvelu (Authentication Service) ja lippupalvelu (Ticket Granting Service). Näiden tehtävänä on todentaa asiakas ja myöntää tälle palvelutikettejä eri palveluihin ja todentaa näin kaksi muuta protokollan osaa toisilleen. Todennuspalvelun ja lippupalvelun ei ole välttämätöntä sijaita samalla

palvelimella, mutta usein näin on. (Gordon 2015, 665.) Kerberos-protokollan osat ja toimintaperiaate on esitetty yksinkertaistettuna kuviossa 2.



KUVIO 2. Kerberos-todennuksen yksinkertaistettu toimintaperiaate (McNab 2016)

Kerberos-todennuksen toimintaperiaatetta voi verrata matkustamiseen, jossa TGT-tiketti (Ticket Granting Ticket) on passi. Passilla voit todistaa, että olet tietyn maan laillinen kansalainen, mutta pelkällä passilla et voi matkustaa toiseen maahan. Matkustamista varten tarvitset myös lentolipun, jonka vastine tässä esimerkissä olisi palvelutiketti (Service Ticket). Kun käyttäjällä on molemmat passi ja tiketti, onnistuu matkustaminen eli tässä tapauksessa tietyn palvelun käyttö.

Kerberos-protokollan etuna on, että käyttäjien salasanoja ei todenneta erikseen palveluihin, vaan niiden sijasta käytetään erillisiä salattuja palvelutikettejä. Tämä mahdollistaa kertakirjautumisen toimialueen käyttäjille, jolloin käyttäjän ei tarvitse kirjautua palveluihin erikseen niin kauan kuin TGT-tiketti on voimassa. Windows AD-ympäristöissä TGT-tiketti myönnetään laitteelle, kun käyttäjä kirjautuu toimialueeseen. (Abernathy & McMillian 2016.)

Kerberoksella on myös heikkoutensa. Se aiheuttaa verkkoon yksittäisen vikaantumispisteen, joka pyritään ehkäisemään asentamalla verkkoon useampia KDC-palvelimia. Windows AD -ympäristöissä kaikki toimialuepalvelimet toimivat oletuksena myös KDC-palvelimina. Kerberoksen heikkous on myös sen perustuvuus salasanoihin,

koska se on tällöin altis salasanan arvaus- ja Brute Force -hyökkäyksille. Lisäksi protokollan tikettejä on mahdollista varastaa tai väärentää. (Gregg 2016.)

Kaikki tiketit jotka kulkevat palvelimen ja asiakkaan välillä aikaleimataan ja niille voidaan määrittää voimassaolo- ja uusiutumisaika. Tämän vuoksi kaikkien verkon laitteiden kellonaikojen on oltava synkronoitu niin, että aikaero on korkeintaan 5 minuuttia (Regan 2014, 385.) Sallittua aikaeroa, sekä tikettien voimassaolo- ja uusiutumisaikoja on kuitenkin mahdollista muuttaa ryhmäpolitiikoiden avulla.

2.1.3 Windowsin kirjautumistietojen tallennuspaikat

Käyttäjän kirjautumistiedot, joita todentamiseen käytetään, on tallennettuna useaan eri paikkaan käyttöjärjestelmässä tilanteesta riippuen. Kirjautumistiedot tallennetaan, jotta kertakirjautuminen ja käyttäjien todentaminen verkossa olisi mahdollista. Näistä tallennuspaikoista tiedot on kuitenkin myös mahdollista varastaa.

Jos kirjautumisen kohde on toimialueen jäsen, on sen kirjautumistiedot tallennettuna toimialuepalvelimen tietokantaan, nimeltä NTDS.DIT. Se on koko toimialueen auktoritatiivinen kirjautumistietojen tallennuspaikka, eli sieltä löytyvät kaikkien toimialueen käyttäjien ja laitteiden käyttäjänimet ja salasanojen tiivisteet. (Jungles ym. 2012, 39.)

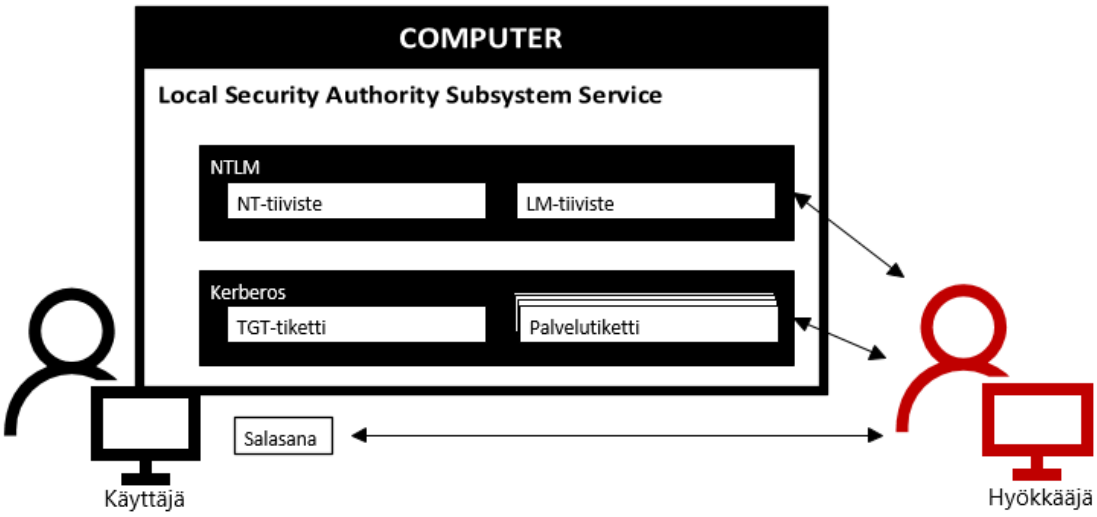
Jos laite taas ei ole toimialueen jäsen, on sen kirjautumistiedot tallennettu tietokoneen paikalliseen SAM-tietokantaan (Security Account Manager). Kyseinen tietokanta on puolestaan paikallisten käyttäjätietojen auktoritatiivinen tallennuspaikka, joka löytyy kaikista Windows-käyttöjärjestelmistä. Tietokantaan on tallennettu kaikki paikalliset tunnukset ja niiden salasanojen NT-tiivisteet. (Jungles ym. 2012, 36.)

Näiden lisäksi kirjautumistiedot tallennetaan aina aktiivisen kirjautumisen ajaksi, paikallisen LSASS-prosessin (Local Security Authority Subsystem Service) muistiin. LSASS on Windows-käyttöjärjestelmän prosessi, jonka vastuulla on käyttöjärjestelmän turvallisuuspolitiikoiden valvonta ja täytäntöönpano. Aktiivisella kirjautumisella tarkoitetaan, että tiedot ovat muistissa, kunnes käyttäjä kirjautuu ulos tai laite uudelleenkäynnistetään. Juuri muistiin tallentamisella mahdollistetaan käyttäjälle

kertakirjautuminen eli yhteys esim. tiedostojakoihin ja sähköposteihin ilman salasanan uudelleensyöttämistä. (Jungles ym. 2012, 37.)

Kirjautumistiedot tallentuvat LSASS-prosessin muistiin paikallisen kirjautumisen lisäksi myös silloin, jos laitteelle kirjaudutaan etätyöpöytäyhteyden avulla tai jos ohjelmia ajetaan toisena henkilönä "RunAs" -optiota käyttäen. Myös ajoitetut tehtävät tai tehtävien ajaminen etätyökalujen, kuten esim. PsExecin avulla aiheuttavat kirjautumistietojen tallentumisen muistiin. (Jungles ym. 2012, 37.)

Tallennettavat kirjautumistiedot sisältävät käyttäjän Kerberos-tiketit, NT- ja/tai LM-tiivisteet, sekä salasanat salattuna. Kuviossa 3 havainnollistetaan samankaltaisuus salasanan, salasanojen tiivisteiden ja Kerberos-tikettien välillä. Hyökkääjä voi siis todentua toisena henkilönä, jos hän saa haltuunsa käyttäjän salasanan, tai minkä tahansa salasanan tiivisteistä tai Kerberos-tiketeistä. (Jungles ym. 2012, 37.)



KUVIO 3. Kirjautumistiedot tallentuvat LSASS:n muistiin (Saydag & Moore 2015)

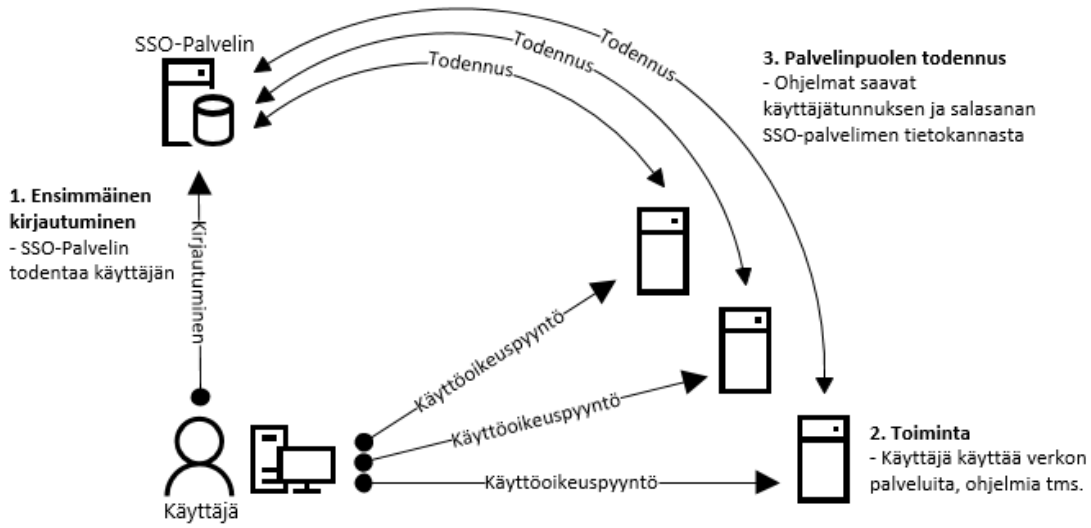
2.2 Kertakirjautuminen (SSO)

Salasanoille asetetaan nykyisin entistä enemmän vaatimuksia ja suosituksia, jotka vaihtelevat käytettävän palvelun mukaan. Yleensä suositellaan, että salasanan tulee pitää sisällään vähintään tietty määrä merkkejä. Lisäksi salasanan pitäisi sisältää numeroita, erikoismerkkejä, pieniä ja isoja kirjaimia. Samaa salasanaa ei myöskään saisi käyttää useassa eri palvelussa, eikä salasanaa saisi löytyä sanakirjasta.

Ajatellaan tilanne, jossa käyttäjä haluaa käyttää toisella palvelimella sijaitsevaa palvelua. Ensiksi käyttäjän pitäisi kirjautua omalle laitteelleen, seuraavaksi verkkoon ja kolmanneksi palvelimelle jossa palvelu sijaitsee ja lopuksi vielä itse palveluun. Jokaiseen näistä olisi oma esim. 15-merkkinen salasanansa ja lisäksi erillinen kirjautumistunnus. Näitä kirjautumistietoja ei myöskään saisi olla kirjoitettuna mihinkään ylös ja ne pitäisi vaihtaa säännöllisin väliajoin.

Tämä tekisi palvelimella olevan palvelun käyttämisestä kohtuuttoman hankalaa, joka johtaisi siihen, että käyttäjät alkaisivat etsiä oikoteitä palvelun käyttämiseen. Tällaisia oikoteitä ovat mm. kirjautumistietojen ylös kirjoittaminen ja salasanojen kierrätys ja yksinkertaistaminen, eli juuri ne asiat joista tietoturva-asiantuntijat käyttäjiä varoittavat. Tämän käytettävyysongelman ratkaisuksi on kehitetty kertakirjautuminen (Single Sign-On). (Gregg 2016.)

Kertakirjautumisella tarkoitetaan, että käyttäjä yhden kerran tunnuksensa ja salasanansa syötettyään pääsee käsiksi kaikkiin resursseihin ja palveluihin, joihin hänellä on oikeus. Tämä tapahtuu ilman, että käyttäjä joutuu kirjautumaan palveluihin uudelleen saman istunnon aikana. Perinteisen kertakirjautumisen arkkitehtuuri ja vaiheet on esitelty kuviossa 4. Kuviossa käyttäjä kirjautuu yhdelle laitteelle, joka todentaa käyttäjän ja jatkossa todennus muille palvelimille tai palveluihin tapahtuu käyttäjän huomaamatta palvelimien välillä.



KUVIO 4. Perinteisen kertakirjautumisen arkkitehtuuri ja vaiheet **(**Gordon 2015, 663)

Jotta kertakirjautuminen olisi mahdollista, täytyy käyttäjän salasanat tallentaa muita kirjautumisia varten tai käyttää tekniikoita, jotka mahdollistavat kertakirjautumisen muilla tavoilla. Esim. salasanojen tallentamista ja syöttämistä skriptien avulla voidaan käyttää, jos käytössä on vanhoja ohjelmistoja, jotka eivät tue uudempia kertakirjautumisen mahdollistavia protokollia. Tällaisten ns. skriptipohjaisten kertakirjautumisjärjestelmien kehitys ja ylläpito on kuitenkin kallista ja niiden tietoturva saattaa jäädä heikoksi. (Gordon 2015, 665.)

Kertakirjautumisen käyttäminen lisää työtehokkuutta ja vähentää inhimillisten virheiden mahdollisuutta. Samalla se vähentää myös verkon ylläpidon työtä, koska käyttäjillä on vähemmän salasanoja muistettavaksi ja unohdettavaksi. Käyttäjät suostuvat myös helpommin käyttämään monimutkaisia salasanoja, jos heillä on muistettavanaan ainoastaan yksi salasana. Kertakirjautumisen käyttäminen mahdollistaa myös keskitetyn ylläpidon ja käyttäjien kirjautumisien paremman valvonnan. (Gordon 2015, 664.)

Kertakirjautumisella on kuitenkin myös heikkoutensa. Se aiheuttaa yksittäisen vikaantumispisteen verkkoon. Tämä tarkoittaa, että kertakirjautumisjärjestelmän kaatuminen voi aiheuttaa sen, ettei kukaan joka järjestelmän palvelua käyttää pääse kirjautumaan mihinkään siihen liitettyyn palveluun. Lisäksi jos hyökkääjä saa käsiinsä kertakirjautumisessa käytettävän salasanan tai sen tiivisteen, on myös hyökkääjällä käytettävissään kaikki palvelut, joihin oikealla käyttäjälläkin on oikeus. **(**Gordon 2015, 664.)

Tätä tilannetta voi havainnollistaa mielikuvalla pankkikortin hukkaamisesta ja verrata sitä ajatukseen koko lompakon hukkaamiseen kerralla. Kertakirjautumisen toteuttaminen eri palveluiden välille voi olla myös hankalaa ja kallista, kun vanhoja ja uusia palveluita pyritään saaman toimimaan yhteen.

3 HYÖKKÄYSKETJUT

3.1 Cyber Kill Chain

Hyökkäysketjulla tarkoitetaan systemaattista prosessia, jossa hyökkäys kohdistetaan ja toteutetaan halutun vaikutuksen aikaansaamiseksi. Termiä ketju käytetään, koska minkä tahansa vaiheen epäonnistuminen, eli ketjun katkeaminen keskeyttäisi koko prosessin. Yhdysvaltojen armeija käyttää prosessista lyhennettä F2T2EA, joka muodostuu sanojen etsi, tunnista, tarkkaile, kohdista, toteuta ja arvioi englanninkielisistä vastineista. (Hutchins, Cloppert & Amin 2011, 4.)

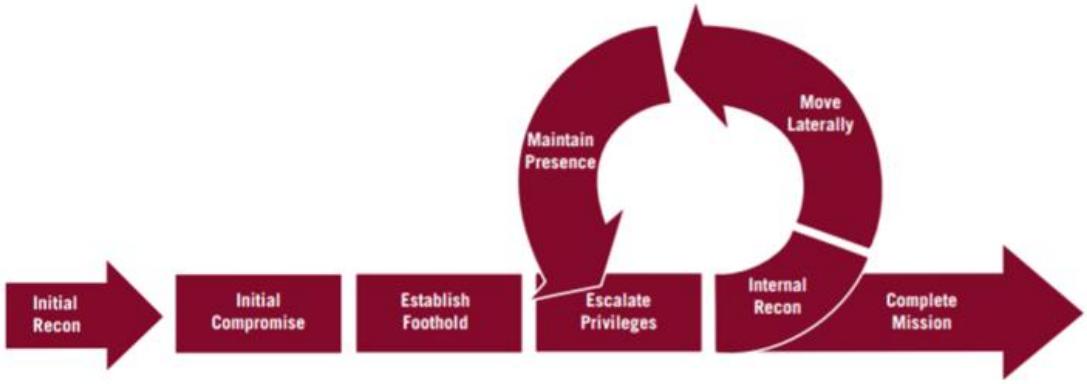
Tätä Yhdysvaltojen armeijan käyttämää 6-vaiheista prosessia pohjana käyttäen kehittivät yhdysvaltalaisen aseteollisuuskonsernin Lockheed Martinin tutkijat kyberhyökkäyksen prosessikaavion vuonna 2009 ja esittelivät sen julkaisussa 2011. Lockheed Martinin 7-vaiheisen kyberhyökkäysketjun vaiheet on esitelty kuviossa 5. (Hutchins ym. 2011, 4; Cloppert 2009.)

KUVIO 5. Lockheed Martinin Cyber Kill Chain (Donaldson, Siegel, Williams & Aslam 2015, 15)

Lockheed Martinin prosessikaaviota on kuitenkin syytetty vanhanaikaiseksi ja tunkeutumiskeskeiseksi. Lisäksi sen on sanottu vahvistavan vanhanaikaista ajattelua siitä, että uhka tulee ainoastaan verkon ulkopuolelta (Engel 2014). Prosessikaavio ei myöskään keskity tarpeeksi siihen, miten hyökkääjä toimii kohdeverkkoon päästyään vaan keskittyy liiaksi tunkeutumista edeltäviin toimiin (Greene 2016).

Lockheed Martinin kaaviosta onkin kehitetty edelleen uusia versioita, jotka kuvaavat yksityiskohtaisemmin moderneja kyberhyökkäyksiä ja hyökkääjän toimia kohdeverkon sisällä. (Donaldson ym. 2015, 16.) Yksi tällainen on Mandiant Attack Life Cycle, joka on esitetty kuviossa 6. Sen julkaisi tietoturvayhtiö Mandiant helmikuussa 2013 osana tutkimustaan Kiinan kansanarmeijan vakoiluyksikkö 61398:sta. Siinä esitellään kiertävänä kehänä hyökkääjän toiminta kohdeverkossa, joka koostuu sisäisestä

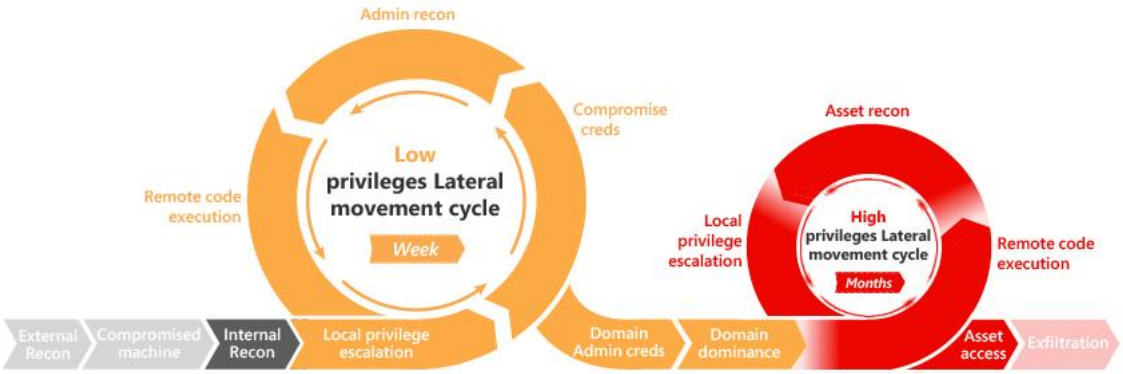
tiedustelusta, lateraalisesta liikkeestä, käyttövaltuuksien laajennuksesta ja kohteessa pysyvyyden varmentamisesta. (Mandiant 2013, 27.)



KUVIO 6. Mandiant Attack Life Cycle (Mandiant 2013, 27)

3.2 Microsoft ATA Kill Chain

Microsoftin GIRR (Global Incident Response and Recovery Team) ja Enterprise Threat Detection Service loivat omien havaintojensa pohjalta oman versionsa kyberhyökkäyksen prosessikaaviosta ja nimesivät sen ATA Kill Chainiksi. Kaavio pohjautuu Mandiantin hyökkäyskaavioon, mutta siinä hyökkäys jaetaan selvemmin kahteen päävaiheeseen, kuten esitetään kuviossa 7. (Trull 2016.)



KUVIO 7. Microsoftin ATA Kill Chain (Microsoft 2016a)

Ensimmäinen päävaihe koostuu sisäisestä tiedustelusta, jossa suoritetaan matalien käyttövaltuuksien lateraalista liikettä ja pyritään levittäytymään kohteessa. Toinen päävaihe alkaa, kun hyökkääjä saa kohdeverkon hallintaansa riittävän korkeiden

käyttövaltuuksien tunnuksien avulla. Tunnuksilla hyökkääjä alkaa suorittaa korkeiden käyttövaltuuksien lateraalista liikettä, etsien päämääräänsä kohdeverkosta.

3.2.1 Ulkoinen tiedustelu ja sisäänpääsy

Ulkoisen tiedustelun vaiheessa hyökkääjä kerää tietoa kohteesta käyttämällä hyväksi julkisesti saatavilla olevaa tietoa. Tähän vaiheeseen kuuluvat esim. kohteen julkisten IP-osoitteiden ja domain-nimien selvittäminen, sekä kohteen työntekijöiden taustojen tutkiminen. Hyökkääjä voi laajentaa tutkimustaan myös kohteen lähipiiriin tai esim. yrityksen alihankkijoihin. Tarkoituksena hyökkääjällä on kerätä mahdollisimman paljon tietoa tulevasta kohteesta ja näin parantaa tulevan hyökkäyksensä onnistumisen mahdollisuutta. Koska kaikki kerätty tieto on julkisesti saatavilla, ei kohde voi tietää siihen kohdistuvasta tiedustelusta. Tämänkaltaisesta tiedustelusta käytetään myös nimitystä passiivinen tiedustelu, koska siinä pyritään välttämään suoraa kontaktia kohteen kanssa (Velazquez 2015, 4).

Kerättyään riittävästi tietoa hyökkääjä pyrkii pääsemään sisään kohdeverkon ensimmäiselle laitteelle. Tässä onnistuakseen hyökkääjä voi toteuttaa esim. tietojenkalastelukampanjoita, joissa kohteen työntekijöille lähetetään sähköpostiviestejä. Näiden viestien liitteenä voi olla haittaohjelman sisältävä liitetiedosto tai linkki huijaussivustolle. Viestit voidaan naamioida uutisviesteiksi, uhrin usein käyttämien palveluiden tai lähipiirin lähettämiksi, jolloin uhri saadaan todennäköisemmin klikkaaman linkkiä tai lataamaan viestin liite. (Mandiant 2013, 63.)

Jos tietojenkalasteluviesti kohdistetaan ja räätälöidään tällä tavalla tietylle henkilölle tai organisaatiolle, on kyse kohdennetusta tietojenkalastelusta (Easttom 2016, 176). Lisäksi jos tietojenkalastelun kohdehenkilö on korkeassa asemassa kohdeorganisaatiossa, käytetään tällaisesta tietojenkalastelusta termiä valastelu. Tämän kaltaiset kohdennetut viestit ovat usein taitavasti väärennetty ja niissä käytetään apuna aiemmin hankittuja tietoja kohteesta ja sen lähipiiristä. Tämän ansiosta kohdennetut hyökkäykset epäonnistuvat vain harvoin. Hyökkääjät ovat kärsivällisiä ja he tietävät, että jossain vaiheessa joku kohdeorganisaatiossa klikkaa aina linkkiä.

Tämä saatiin huomata myös suomalaisen tietoturvayhtiö F-Securen Red Teamin asiakasorganisaatioon tekemässä testissä, jossa asiakasorganisaation työntekijöistä 52% klikkasi LinkedIn-viestiksi naamioidun huijausviestin linkkiä. Saman testin toisessa osassa viestin vastaanottajia pyydettiin täyttämään tunnuksensa ja salasanansa linkin takana olevaan portaaliin. 13% asiakasorganisaation työntekijöistä lankesi huijausviestiin ja erehtyi syöttämään kirjautumistietonsa huijaussivulle. (Karkimo 2017.)

Tietojenkalastelu sähköpostitse ei kuitenkaan ole ainoa keino jolla hyökkääjä voi yrittää päästä sisään kohdeverkkoon. Hyökkääjä voi myös soittaa yritykseen ja toteuttaa käyttäjän manipulointiin perustuvia huijauksia tai hyökkääjä voi toimittaa haittaohjelman kohteeseen vaikkapa kohdeyrityksen alihankkijoiden mukana tai jollain muulla tavalla.

3.2.2 Sisäinen tiedustelu

Kun hyökkääjä lopulta pääsee sisään ensimmäiselle kohdeverkon laitteelle, pyrkii se usein ensimmäiseksi varmistamaan jalansijansa kohdeverkossa. Tämä tapahtuu asentamalla takaovia tai VPN-yhteyksiä (Virtual Private Network) kohteeseen. Yleensä palomuurit estävät verkon ulkopuolelta tulevan liikenteen pääsyn sisäverkkoon, mutta eivät sisäverkosta ulospäin. Takaovia asentamalla hyökkääjän on mahdollista ajaa etäkomentoja omalta hallintapalvelimeltaan, koska pyynnöt verkkoliikenteelle tulevat sisäverkon puolelta. (Mandiant 2013, 63.)

Sisään kohdeverkkoon päästyään hyökkääjä pyrkii myös nopeasti varmistumaan siitä, ettei haltuun saatu laite ole hiekkalaatikko (sandbox) tai houkutuslaite (honeypot), joita käytetään tietoturvatutkimuksessa ja osana kyberpuolustusta. Tämän varmentamisessa ja haltuun saadun laitteen tutkimisessa hyökkääjä käyttää hyväkseen käyttöjärjestelmässä valmiina olevia komentoja, kuten *tasklist, ver* ja *systeminfo* (Tomonaga 2016).

Varmistuttuaan kohteen aitoudesta, hyökkääjä alkaa kerätä tietoa, jota ei ole ollut saatavilla ulkopuolelta käsin. Hyökkääjä tutkii saastuneen laitteen saatavilla olevat paikalliset levyt, verkkojaot, Sharepoint- ja wiki-sivustot, sekä etsii verkosta muita laitteita, erityisesti DNS- ja toimialuepalvelimia. (Mandiant 2013, 64.) Lisäksi hyökkääjä pyrkii selvittämään kohdeverkon käyttäjätilejä ja -ryhmiä komennoilla kuten *net user* ja *net group* (Tomonaga 2016).

Hyökkääjä voi myös ladata laitteeseen ulkopuolisia ohjelmistoja, kuten Mimikatz ja Netsess tiedonkeruutaan varten. Mimikatzin avulla hyökkääjä voi etsiä laitteen muistista käyttäjätunnuksia, salasanoja tai salasanojen tiivisteitä ja Kerberos-tikettejä. Näiden tietojen avulla hyökkääjä voi myöhemmin levitä verkossa. Netsessin avulla hyökkääjä voi puolestaan tarkistaa mitkä käyttäjätilit ovat aktiivisina missäkin IP-osoitteessa. Tämä tapahtuu luetteloimalla NetBIOS-sessioita toimialuepalvelimelle. (Harris, Zilberstein & Zinger 2017, 18.)

Näiden lisäksi hyökkääjä voi asentaa kohdelaitteelle myös muita ohjelmia, kuten esim. näppäimen painallukset tallentavia haittaohjelmia. Ohjelmien siirrossa laitteelle hyökkääjä käyttää yleensä omia komento- ja kontrollipalvelimiaan.

3.2.3 Leviäminen

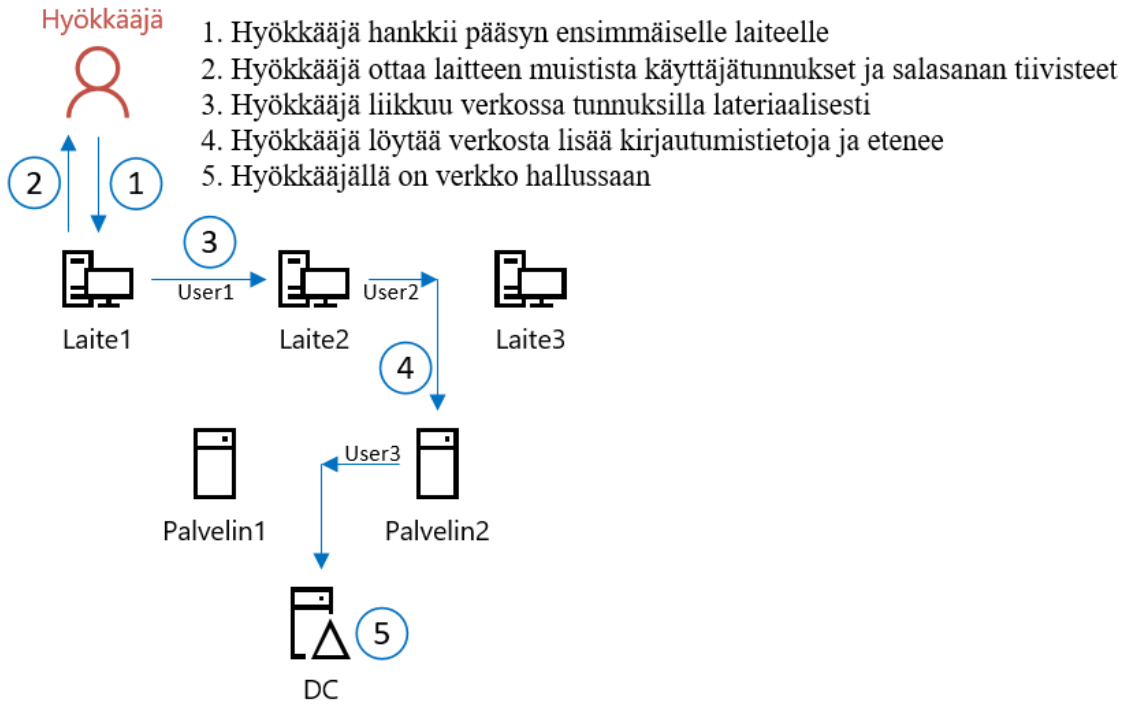
Useimmissa tapauksissa ensimmäinen saastunut laite ei sisällä sitä mitä hyökkääjä on tullut hakemaan. Tällöin hyökkääjä pyrkii leviämään kohdeverkossa. Tätä vaihetta kuvataan lateraaliseksi liikkeeksi, jolla tarkoitetaan, että hyökkääjä liikkuu verkossa samanarvoisten laitteiden ja tunnusten välillä. Lateraalista liikettä on esim. että hyökkääjä varastaa yhden laitteen oletustunnuksen ja salasanan ja käyttää niitä kirjautuakseen toiseen laitteeseen, joka käyttää samaa oletustunnusta ja salasanaa. (Jungles ym. 2012, 9.) Lateraalisen liikkeen tarkoituksena on levittäytyä ja varmistaa pysyvyys kohdeverkossa (Mandiant 2013, 64).

Hyökkääjä voi liikkua verkossa esim. Overpass-the-Hash tai Pass-the-Ticket -hyökkäyksien avulla, jolloin hyökkääjä näyttää verkossa samalta kuin normaalikäyttäjä. Tällaisen liikenteen erottaminen on vaikeaa ja hyökkääjä pystyy liikkumaan verkossa huomaamattomana pidempään. (Mandiant 2013, 64.) Hyökkääjä voi kuitenkin yrittää päästä varastamillaan tunnuksilla käsiksi tietoihin joihin niillä ei ole oikeutta, mikä saattaa aiheuttaa hälytyksen kohdeverkon valvontajärjestelmissä.

Hyökkääjä käyttää liikkumisessa apuna myös etätyöpöytä-protokollia, kuten RDP (Remote Desktop Protocol). Lisäksi hyökkääjä voi käyttää sisäänrakennettuja komentoja kuten *at* ja *wmic*, sekä ladattavia etätyökaluja kuten PsExec apuna suorittaakseen ohjelmiaan etänä muissa verkon laitteissa. (Tomonaga 2016; Mandiant 2013, 36.)

Verkossa liikkuessaan hyökkääjän tavoitteena on saada itselleen enemmän valtuuksia. Tässä käyttövaltuuksien laajentamisvaiheessa hyökkääjä pyrkii hankkimaan jollekin käyttämälleen tunnukselle enemmän oikeuksia, kuin sille on tarkoitettu tai löytämään jonkun toisen laitteen muistista laajempien käyttövaltuuksien tunnukset. Hyökkääjä voi esim. varastaa työasemalta palvelimen ylläpitäjän tunnukset, jos ylläpitäjä kirjautuu etänä työasemalle. Olemassa olevien tunnusten oikeuksien korotus puolestaan tapahtuu yleensä verkon suunnitteluvirheen tai ohjelmistoissa olevien ohjelmointivirheiden avulla. (Jungels ym. 2012, 9; Mandiant 2013, 64.)

Leviämisvaiheessa hyökkäyksessä kyse on siis lopulta laajempien valtuuksien hankkimisesta kohdeverkkoon. Näiden valtuuksien avulla hyökkääjä voi edetä kohdeverkossa kohti paremmin suojattuja resursseja. Hyökkääjä siirtyy laitteesta toiseen, kunnes saa korotettua tunnustensa oikeudet tai löytää kohdeverkosta riittävät tunnukset. Tällaiset valtuudet saatuaan hyökkääjä voi ottaa koko verkon hallintaansa. Tämä leviämisprosessi on esitetty yksinkertaistettuna kuviossa 8.



KUVIO 8. Hyökkääjän liike kohdeverkossa (Jungles ym. 2012, 13)

3.2.4 Hallinta ja haluttu toiminta

Jos hyökkääjä saa haltuunsa toimialueen ylläpitäjän tai vastaavan tason tunnukset, on hänellä koko toimialue hallinnassaan. Hyökkääjä pystyy silloin ajamaan ohjelmia, luomaan käyttäjiä ja määrittämään käyttöoikeuksia kohdeverkossa samoin kuin verkon ylläpitäjät. Tämä vaarantaa myös muut toimialueet jotka luottavat hyökkääjän haltuun saamaan toimialueeseen. Hyökkääjä voi myös pyrkiä varmistamaan pääsynsä jatkossakin kohdeverkkoon esim. Golden Ticket tai Skeletonkey -hyökkäysten avulla. Näiden hyökkäysten avulla hyökkääjä voi luoda yleisavaimen kaikkiin verkon tunnuksiin tai väärentää itselleen Kerberos-protokollassa käytettyjä TGT-tikettejä.

Kun hyökkääjällä on verkko hallussaan, pyrkii se löytämään ja pääsemään käsiksi haluamiinsa resursseihin tai suorittamaan muun haluamansa toiminnan kohdeverkossa. Yleensä tällä tarkoitetaan yrityksen tai organisaation tietojen varastamista, tuhoamista tai salaamista, mutta lopulta toiminta riippuu aina hyökkääjästä ja mitkä hänen tavoitteensa ja motiivinsa ovat.

Jos hyökkääjä pyrkii varastamaan tietoa, siirtää hän varastetun datan kohdeverkosta itselleen yleensä pakattuna ja salattuna. Siirtämiseen hyökkääjä voi käyttää esim. FTP- (File Transfer Protocol) ja SFTP-protokollia (SSH File Transfer Protocol) tai internetpohjaisia tiedonsiirtopalveluja. Hyökkääjä saattaa myös pilkkoa pakkaamansa datan osiin ennen lähetystä. (Mandiant 2013, 37, 65.)

4 KEHITTYNEET UHAT

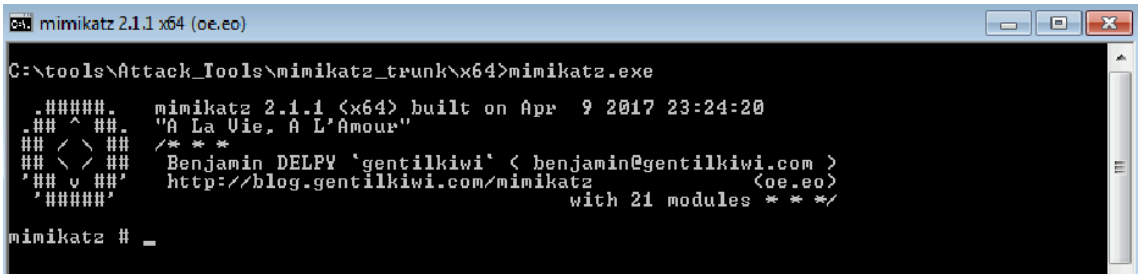
4.1 Mimikatz

Mimikatz on avoimen lähdekoodin työkalu, jota käytetään myöhäisessä vaiheessa tunkeutumista eli sitten kun kohdeverkkoon on jo päästy sisään. Sen avulla on mahdollista mm. varastaa käyttäjien kirjautumistietoja LSASS-prosessin muistista ja syöttää niitä edelleen toteuttaakseen hyökkäyksiä kuten Pass-the-Hash ja Pash-the-Ticket.

Ranskalainen Benjamin Delpy aloitti ohjelman tekemisen jo vuonna 2007 opetellakseen paremmaksi ohjelmoijaksi ja hän kehittää ohjelmaa yhä. Mimikatz on itsenäinen ohjelmisto, mutta sen toiminnot ovat saatavilla myös osana Meterpreter ja PowerSploit tunkeutumisen testausohjelmistoja. (Delby 2014.)

Suurin osa virustorjuntaohjelmistoista tunnistaa nykyään Mimikatzin haitalliseksi. Tämä ei kuitenkaan juuri tarjoa suojaa ohjelman toiminnoilta, sillä ohjelman lähdekoodi on vapaasti saatavissa. Tästä johtuen kuka tahansa voi muokata ohjelmasta uusia versioita, joita virustorjuntaohjelmat eivät välttämättä tunnista. Lisäksi hyökkääjä voisi kohdelaitteelle päästyään yksinkertaisesti sulkea virustorjuntaohjelmiston tai asettaa sen olemaan huomioimatta Mimikatz-ohjelmaa.

Mimikatz käynnistetään komentoriviltä komennolla Mimikatz.exe, joka avaa ohjelman käyttöliittymän. Mimikatzin version 2.1.1 käyttöliittymä on esitetty kuvassa 1.



KUVA 1. Mimikatz-ohjelman komentoliittymä

Mimikatzin käyttöliittymä on pelkkä komentoliittymä ilman graafisia elementtejä. Ohjelmaan voidaan syöttää komentoja, joko ensin ohjelman käynnistämällä tai sitten

suoraan Windowsin komentokehotteelta. Windowsin komentokehotteelta komentojen syöttäminen tapahtuu ketjuttamalla komennot ja lisäämällä loppuun ”exit”, jos haluaa komentojen jälkeen palata takaisin komentokehotteeseen. Alla esimerkki komentojen ketjuttamisesta ja taulukko 2, johon on listattu yleisimpiä Mimikatz-ohjelman komentoja ja niiden toiminnot.

```
Mimikatz.exe ”<komento>” ”<komento>” ”<...>” ”exit”
```

TAULUKKO 2. Mimikaz-ohjelmiston yleisiä komentoja (Metacalf 2016)

Komento:	Selite:
CRYPTO::Certificates	Listaa/vie sertifikaatit
KERBEROS::Golden	Luo Golden/Silver -tikettejä
KERBEROS::List	Listaa kaikki käyttäjien tiketit muistista
KERBEROS::PTT	Pass-the-Ticket
LSADUMP::DCSync	Synkronoi objekti DC:lle (pyydä salasanaa tilille)
LSADUMP::LSA	Vie kaikki AD:n pääsytiedot tiedostoon
LSADUMP::SAM	Vie kaikki paikalliset pääsytiedot tiedostoon
MISC::Skeleton	Injektoi Skeletonkey LSASS-prosessiin
PRIVILEGE::Debug	Ota käyttöön debug-oikeudet
SEKURLSA::Ekeys	Listaa Kerberoksen salausavaimet
SEKURLSA::Kerberos	Listaa Kerberos kirjautumistiedot käyttäjille
SEKURLSA::Krbtgt	Listaa KRBTGT-tilin salasanatiedot
SEKURLSA::LogonPasswords	Listaa kaikki saatavilla olevat kirjautumistiedot
SEUKRLSA::Pth	Pass-the-Hash ja Overpass-the-Hash
SEKURLSA::Tickets	Listaa kaikki saatavilla olevat Kerberos-tiketit

4.2 Menetelmät

4.2.1 Tiedustelu

Kuten aiemmin mainittu, tiedustelua suorittaessaan hyökkääjä käyttää apuna kohdelaitteen käyttöjärjestelmään sisäänrakennettuja työkaluja ja komentoja. Esim. tällaisesta työkalusta on Nslookup. Nslookup on DNS-kyselytyökalu, jonka avulla

voidaan selvittää, mikä IP-osoite vastaa mitäkin toimialueen nimeä tai toisinpäin mikä nimi vastaa mitäkin IP-osoitetta. Työkalun avulla hyökkääjä voi toteuttaa kohdeverkossa DNS-tiedustelua huomaamattomasti. Taulukossa 3 on listattu Japanin CERTin (Computer Emergency Response Team) useimmiten havaitsemia Windows-komentoja, joita on käytetty varhaisessa vaiheessa kyberhyökkäystä, sekä niiden toiminnot.

TAULUKKO 3. Komennot varhaisessa vaiheessa (Tomonaga 2016; Technet 2015)

Komento:	Toiminto:
tasklist	Listaa käynnissä olevat ohjelmat ja palvelut
ver	Näyttää Windowsin versionumeron
ipconfig	Näyttää TCP/IP-verkkoasetukset
systeminfo	Näyttää yksityiskohtaista tietoa laitteesta ja käyttöjärjestelmästä
net time	Synkronoi tai näyttää toisen laitteen kellonajan
netstat	Näyttää aktiiviset TCP-yhteydet, portit yms.
whoami	Näyttää nykyisen käyttäjän ja toimialueen nimen
net start	Käynnistää palvelun tai listaa käynnissä olevat palvelut
query	Käytetään tietojen katseluun mm. käyttäjä, sessio, prosessi

Muita hyökkääjän käyttämiä käyttöjärjestelmäkomentoja, joiden käyttö ei herätä epäilyksiä perinteisissä tietoturvaratkaisuissa, on listattu taulukossa 4. Näitä komentoja voidaan käyttää esim. käyttäjien ja ryhmien luettelointiin. Huomion arvoista kuitenkin on, että komentojen toimintoihin voidaan vaikuttaa niille syötettävien parametrien avulla.

TAULUKKO 4. Komennot tiedusteluvaiheessa (Tomonaga 2016; Technet 2015)

Komento:	Toiminto:
dir	Listaa kansion tiedostot
net view	Listaa toimialueresurssit joihin voidaan yhdistää
ping	Käytetään yhteyden testaamiseen laitteiden välillä
net use	Käytetään resurssien käyttämiseen
type	Näyttää tiedostojen sisällön, käytetään myös etsintään
net user	Hallitaan lokaaleja ja toimialuetilejä
net group	Listaa käyttäjät jotka kuuluvat tiettyyn toimialueryhmään
net config	Listaa palveluita joita voidaan muokata
net share	Käytetään jaettujen resurssien hallintaan

Yleensä hyökkääjä on luonut valmiiksi skriptejä nopeuttaakseen tiedusteluaan. Kuvassa 2 on esitetty esimerkki skriptistä, johon toiminnot on kommentoitu selkeyden vuoksi. Tämänkaltaista tiedusteluskriptiä käytti Mandiantin (2013, 35.) mukaan myös kiinalainen valtiollinen vakoiluyksikkö ainakin neljässä kyberhyökkäyksessään. Skripti mahdollistaa hyökkääjälle laitteen ja sen toimialueen tietojen keräämiseen yhteen tekstitiedostoon nopeasti.

```
@echo off

::Luo kansio c:\temp
mkdir c:\temp
::IP-asetukset
ipconfig /all>>"C:\temp\Info.txt"
::Käynnissa olevat Windows-palvelut
net start>>"C:\temp\Info.txt"
::Käynnissa olevat prosessit
tasklist /v>>"C:\temp\Info.txt"
::Järjestelmän käyttäjätilit
net user >>"C:\temp\Info.txt"
::Järjestelmän paikalliset pääkäyttajät
net localgroup administrators>>"C:\temp\Info.txt"
::Aktiiviset TCP-yhteydet
netstat -ano>>"C:\temp\Info.txt"
::Laitteet nykyisessa toimialueessa
net view>>"C:\temp\Info.txt"
::Toimialueet verkossa
net view /domain>>"C:\temp\Info.txt"
::Globaalit ryhmät toimialueessa
net group /domain>>"C:\temp\Info.txt"
::"Domain users" -ryhmän jäsenet
net group "domain users" /domain>>"C:\temp\Info.txt"
::"Domain admins" -ryhmän jäsenet
net group "domain admins" /domain>>"C:\temp\Info.txt"
::"Domain controllers" -ryhmän jäsenet
net group "domain controllers" /domain>>"C:\temp\Info.txt"
::"Exchange domain servers" -ryhmän jäsenet
net group "exchange domain servers" /domain>>"C:\temp\Info.txt"
::"Exchange servers" -ryhmän jäsenet
net group "exchange servers" /domain>>"C:\temp\Info.txt"
::"Domain computers" -ryhmän jäsenet
net group "domain computers" /domain>>"C:\temp\Info.txt"
```

KUVA 2 Esimerkki tiedusteluskriptistä (Mandiant 2013, 35)

4.2.2 Pass-the-Hash (PtH)

PtH on yksi variaatio käyttäjätunnusvarkaustekniikoista, joilla pyritään esiintymään verkossa toisena henkilönä. Tarkemmin kuvattuna PtH:lla tarkoitetaan hyökkäystä, jossa laitteen muistiin tallennettu käyttäjätunnus ja salasanan tiiviste varastetaan ja niiden avulla todennutaan kohdeverkossa toisena henkilönä. (Jungles ym. 2012, 6.)

Kun hyökkääjällä on käyttäjän tunnus ja salasanan tiiviste, on hänellä käytössään kaikki samat oikeudet ja resurssit verkossa, kuin tunnuksen oikealla omistajalla. Hyökkääjän ei siis tarvitse tietää käyttäjän salasanaa vaan riittää, että hyökkääjä saa haltuunsa pelkän salasanan tiivisteen. (Easttom 2016, 149.)

PtH kuten muutkin käyttäjätunnustenvarkauksiin liittyvät hyökkäykset, ovat usein kaksivaiheisia. Ensiksi hyökkääjän tulee päästä käsiksi vähintään yhden laitteen paikallisiin pääkäyttäjän tunnuksiin, jotta hyökkääjä voisi niiden avulla varastaa muiden käyttäjien tunnuksia ja salasanojen tiivisteitä laitteelta. (Jungles ym. 2012, 8.)

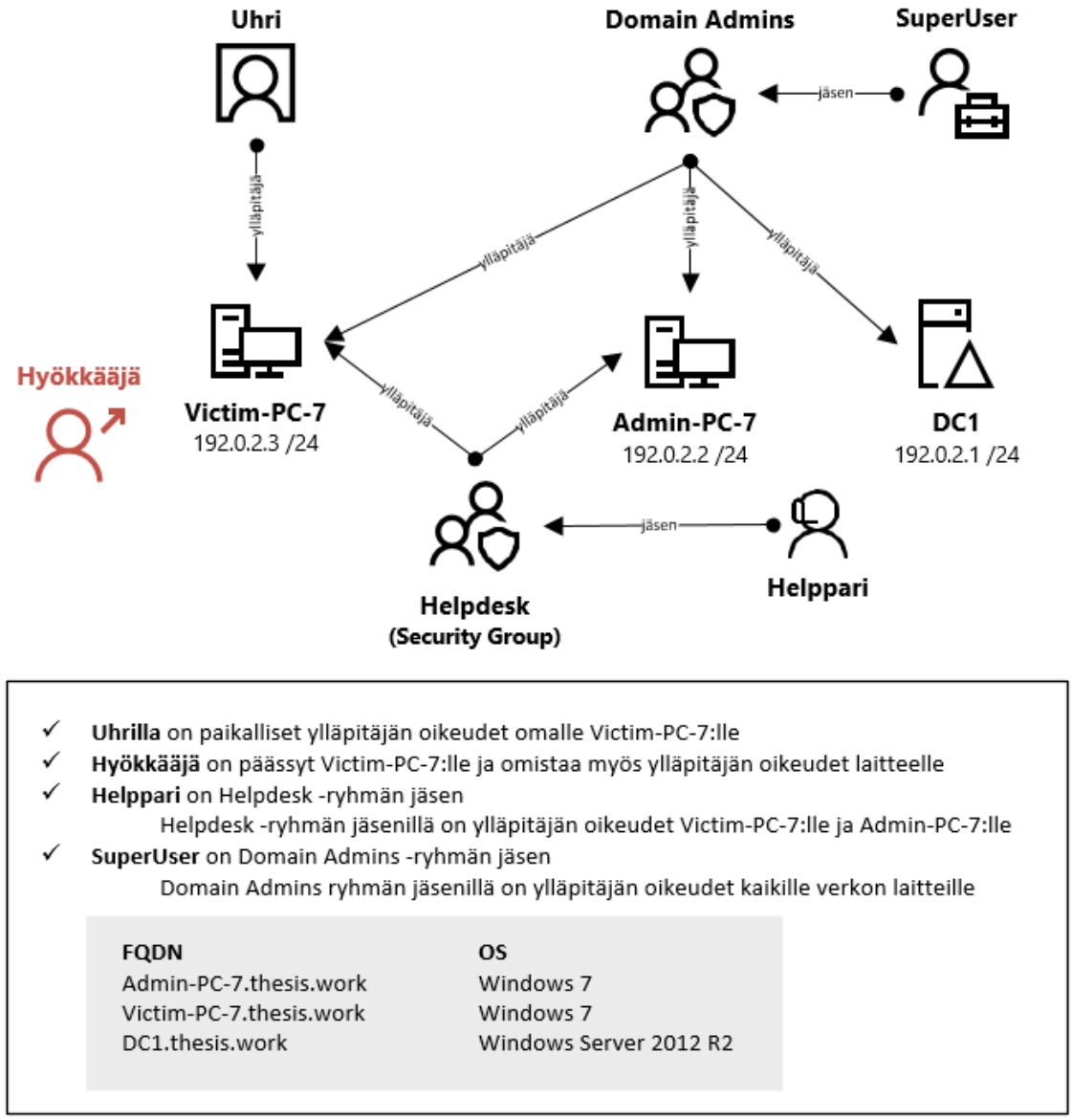
Toiseksi hyökkääjä pyrkii käyttämään varastamiaan tunnuksia päästäkseen käsiksi muihin verkon laitteisiin, joista hyökkääjä voi varastaa lisää kirjautumistietoja ja näin edetä kohdeverkossa kohti haluamiaan resursseja. Huomionarvoista on, että varastettavilla käyttäjätunnuksilla on oltava kirjauduttu kohdelaitteeseen, eli esim. toimialueen käyttäjän tunnuksia, joilla ei ole koskaan kirjauduttu kohdelaitteelta, ei voida kohdelaitteelta tällä tavoin myöskään varastaa. (Jungles ym. 2012, 8.)

Varastettavien tunnusten ei kuitenkaan tarvitse olla käyttäjätilin, vaan myös palvelu- tai laitetilin tiedot voidaan varastaa. Kirjautumistietojen varastaminen tapahtuu Mimikatzin, Windows Credential Editorin tai jonkun muun vastaavan "Credential Dumping" -työkalun avulla. (Jungles ym. 2012, 8.)

Esimerkki

Luodaan esimerkkitilanne, jossa on kolme laitetta, kolme käyttäjää, kaksi käyttäjäryhmää ja hyökkääjä. Esimerkkiä varten luotu verkkoympäristö ja sen käyttäjät on kuvattu kuviossa 9. Esimerkkiympäristö on rakennettu Hyper-V -virtualisointialustan päälle ja samaa ympäristöä käytetään kaikkien hyökkäysmenetelmien esimerkeissä. Ympäristö

perustuu Microsoftin Advanced Threat Analytics Attack Simulation Playbook -julkaisussa esiteltyyn ympäristöön. (Harris ym. 2017, 11.)



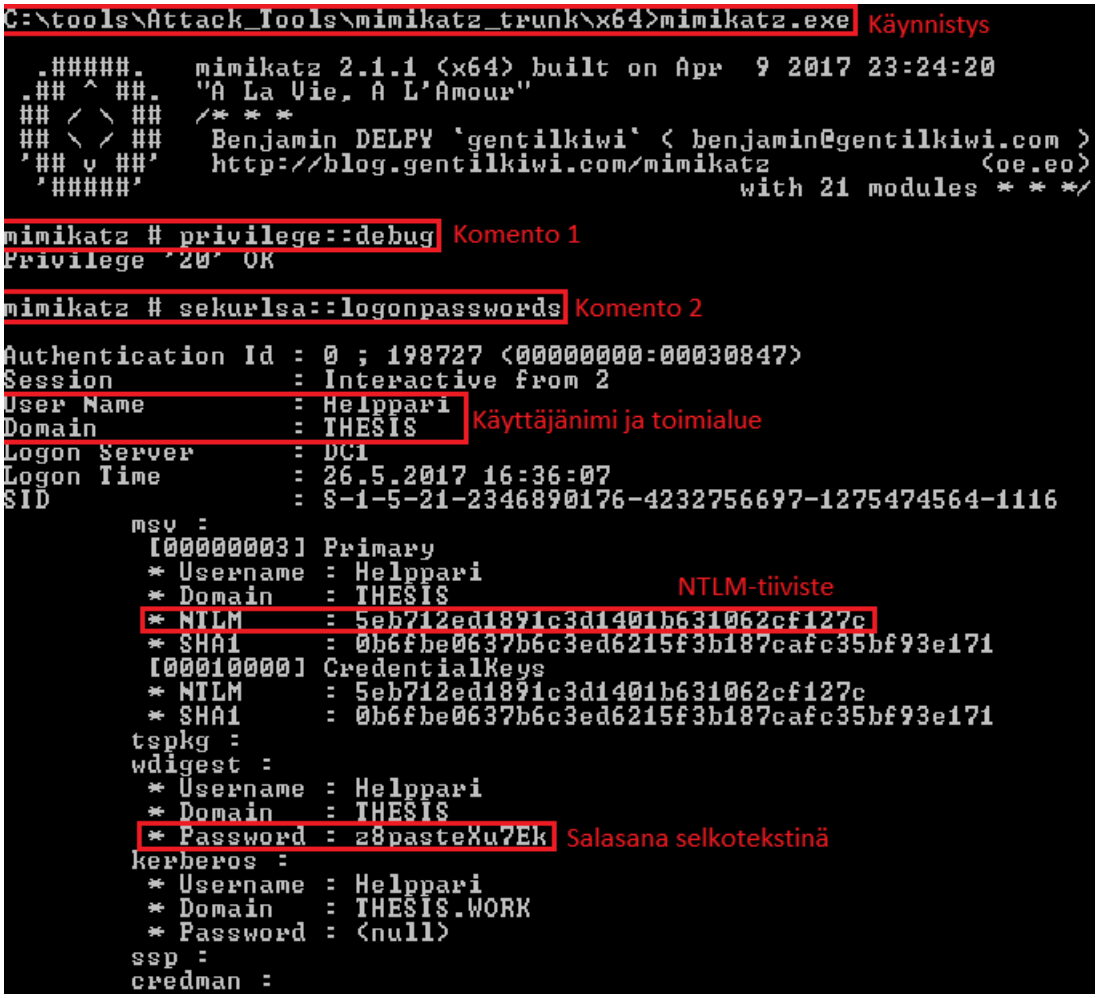
KUVIO 9. Menetelmien esimerkeissä käytettävä verkkoympäristö

Esimerkissä IT-tuki (Helppari) kirjautuu etänä laitteelle (Victim-PC-7), johon hyökkääjä on jo aiemmin päässyt sisään. Kun IT-tuki kirjautuu laitteelle jäävät hänen kirjautumistiedot LSASS-prosessin muistiin aktiivisen yhteyden ajaksi. Tiedot ovat muistissa, kunnes IT-tuki kirjautuu ulos tai laite uudelleenkäynnistetään. Tämä tarkoittaa, että jos IT-tuki esim. sulkee etäyhteyden ikkunan kirjautumatta ensin ulos, jäävät hänen kirjautumistunnuksensa toisen laitteen muistiin. Hyökkääjä voi tällöin esim. Mimikatzin avulla varastaa IT-tuen tunnuksen ja salasanan tiivisteen tai joissain tapauksissa jopa selkotekstisen salasanan laitteen muistista. Esimerkkitilanteen alussa hyökkääjä on jo ladannut Mimikatzin ja muuta tarvittavat ohjelmat uhrin laitteelle.

Mimikatzin käynnistämisen jälkeen kirjautumistiedot saadaan näkyviin laitteen muistista kahdella komennolla, joista ensimmäinen määrittelee ohjelmalle debug-oikeudet ja toinen listaa kirjautumistunnukset muistista:

```
Privilege::debug
Sekurlsa::logonpasswords
```

Kuvassa 3 komennot on suoritettu ja kuvassa on nähtävissä etänä kirjautuneen IT-tuen ”Helppari” -käyttäjätunnus, käytössä oleva toimialue ”Thesis.work”, salasanan NTLM-tiiviste, sekä tällä kertaa myös salasana selkotekstinä laitteen muistista noudettuna.



KUVA 3. Mimikatzillä noudetut kirjautumistiedot, joissa salasana näkyvissä

Salasana oli saatavilla selkotekstinä, koska esimerkkiverkossa ei ole estetty Wdigestin käyttöä. Wdigest on Windowsiin sisäänrakennettu todennusominaisuus, joka mahdollistaa automaattisen todentumisen web-palveluihin jotka käyttävät Digest-todennusta. Tätä automaattista todennusta varten Windows säilyttää käyttäjän salasanasta

selkotekstistä versiota muistissaan. Wdigest on oletuksena pois päältä Windows 8.1 ja Server 2012 R2 käyttöjärjestelmistä eteenpäin, mutta esimerkissämme käytössä on Windows 7, jolloin Wdigestin käyttö täytyy erikseen estää. (Falde 2014.) Wdigest voidaan poistaa käytöstä ja samalla estää selkotekstisen salasanan tallentuminen muistiin lisäämällä Windowsin rekisterisijaintiin:

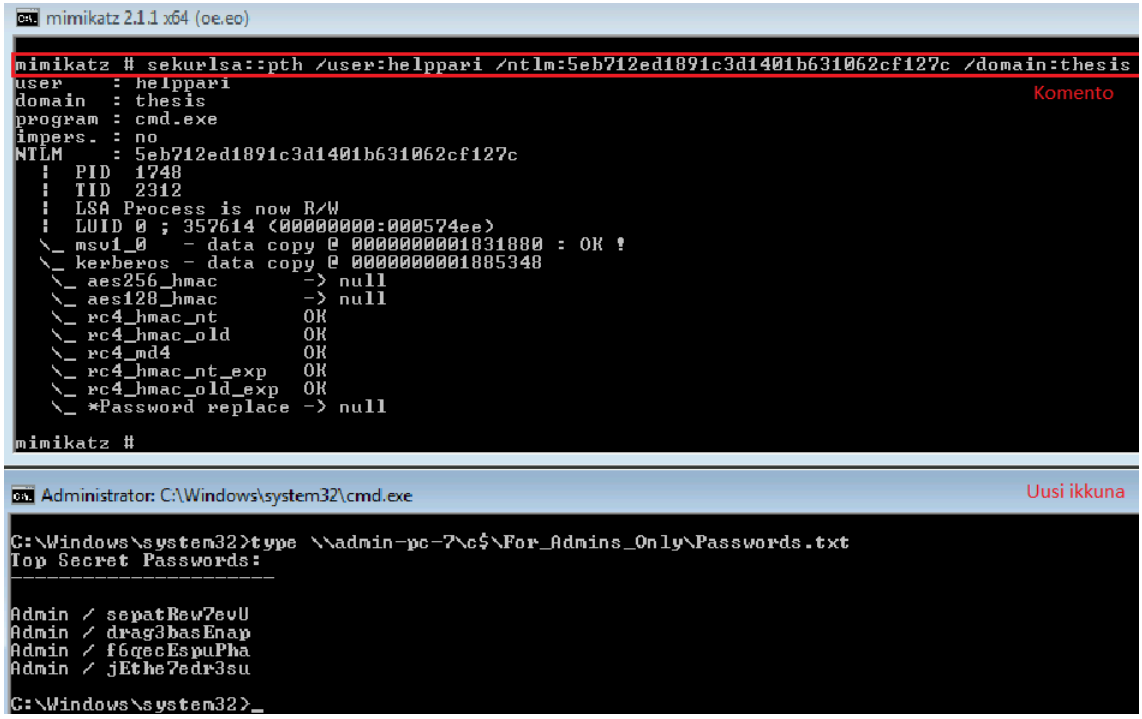
```
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/
SecurityProviders/WDigest/
```

`UseLogonCredential` -merkintä ja asettamalla sen arvoksi `0`. Tämän lisäksi laite on uudelleenkäynnistettävä. (Falde 2014.)

Vaikka selkotekstistä salasanaa ei saisikaan esiin laitteen muistista, saa hyökkääjä kuitenkin riittävät tiedot joilla voi todentaa itsensä. Tähän riittävät toimialueen nimi, käyttäjänimi ja salasanan tiiviste. Nämä kirjautumistiedot voidaan syöttää Mimikatzin komennoilla:

```
”Sekurlsa::pth /user:Helppari
/ntlm:5eb712ed1891c3d1401b631062cf127c /domain:thesis”
```

Tämä komento avaa uuden ikkunan, jossa hyökkääjällä on IT-tuen tunnuksen käyttöoikeudet. Tästä ikkunasta hyökkääjä pääsee käsiksi resursseihin esim. toisella laitteella olevaan kansioon johon vain IT-tuella on käyttöoikeus. Kuvassa 4 aiemmin saadut kirjautumistiedot on syötetty Mimikatziin, jolloin uusi ikkuna on auennut. Tässä uudessa ikkunassa on avattu toisella laitteella (Admin-PC-7) sijaitsevan ”Passswords.txt” tiedoston sisältö, vaikka hyökkäyksen ensimmäisen kohteen käyttäjällä (Uhri) ei pitäisi olla siihen oikeutta.



KUVA 4. Kirjautumistietojen syöttäminen Mimikatzillä ja esim. PtH:sta

4.2.3 Overpass-the-Hash

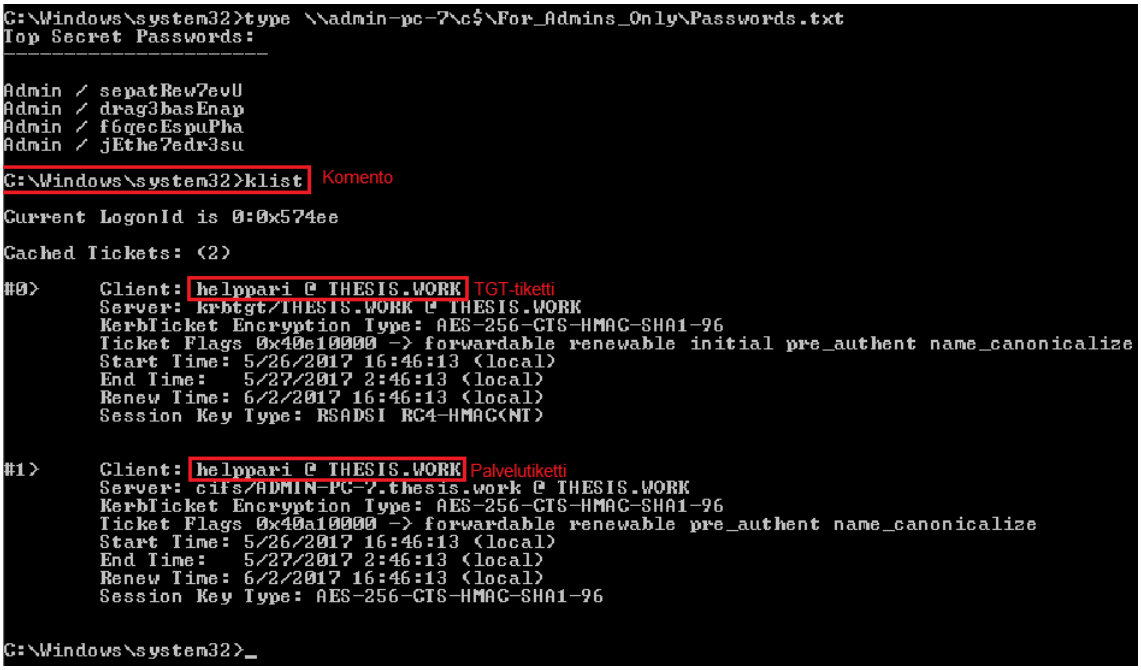
Overpass-the-Hash josta joskus käytetään myös nimeä Pass-the-Key, on hyvin samankaltainen hyökkäys kuin Pass-the-Hash. Erona on, että NTLM-tiivisteellä todentumisen sijaan tarkoituksensa on käyttää NTLM-tiivistettä, jotta saadaan toisen käyttäjän Kerberoksen TGT-tiketti varastettua, jonka avulla sitten voidaan todentua. Tähän tarkoitukseen voidaan NTLM-tiivisteen lisäksi käyttää myös käyttäjän AES-avainta, joka saataisiin näkyviin kohdelaitteen muistista Mimikatzin komennolla:

```
Sekurlsa::ekeys
```

Esimerkki

Aikaisemmassa esimerkissä saatiin Mimikatzillä esiin IT-tuen (Helppari) käyttäjätunnus ja NTLM-tiiviste (5eb712ed1891c3d1401b631062cf127c). Nämä kirjautumistiedot syötettiin Mimikatzille ja päästiin käsiksi resursseihin toisella laitteella (Admin-PC-7) joihin käyttäjällä ei ollut oikeutta. Klist-komennon avulla voidaan tarkastella mitä Kerberos-tikettejä laitteen muistissa on. Kuvassa 5 klist-komento on suoritettu ja kuvasta voimme havaita, että käytössä on ”Helppari” -tilin Kerberos-tiketit. Edellinen PtH-hyökkäyksemme oli itse asiassa samaan aikaan Overpass-the-Hash -hyökkäys. Tämä

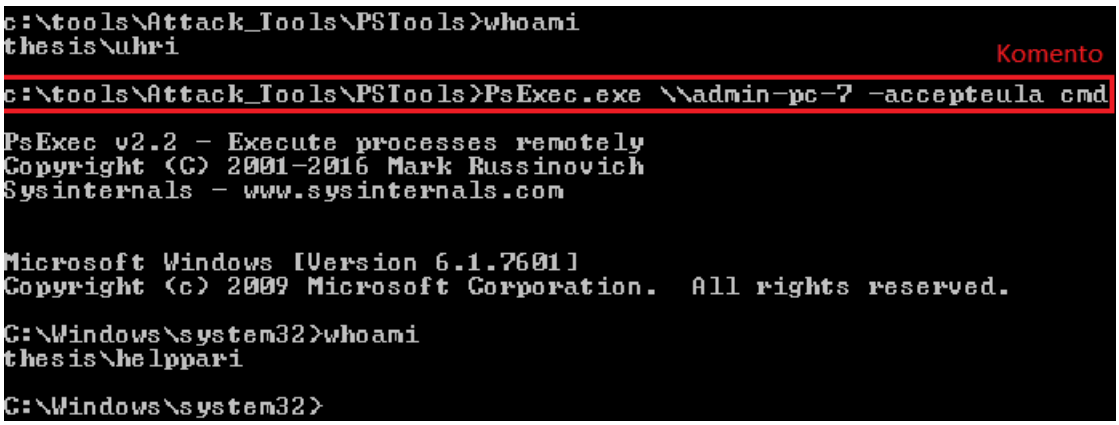
johtuu siitä, että esimerkkiverkkomme laite oli toimialueen jäsen, jolloin siinä oli käytössä Kerberos-todennus.



KUVA 5. Overpass-the-Hash -hyökkäyksellä varastetaan toisen käyttäjän TGT-tiketti

Overpass-the-Hash -hyökkäys onnistuu, koska käyttäjän normaalisti todistaessa Kerberoksen KDC-palvelimelle henkilöllisyytensä, salaa laite sen hetkisen kellonajan ja lähettää sen ensimmäisen viestin mukana KDC-palvelimelle. Kellonaika vaaditaan, jotta palvelin tietää laitteiden kellonaikojen olevan riittävän lähellä toisiaan ja lisäksi sitä käytetään protokollassa ns. PREAUTH-viestinä. KDC-palvelin viestin saatuaan tarkistaa käyttäjän henkilöllisyyden ja lähettää TGT-tiketin käyttäjälle. Kerberos-protokollan hyväksymät salausalgoritmit Windows 8.1 asti sisältävät kuitenkin oletuksena AES-salauksen lisäksi myös RC4-HMAC-salauksen, joka käyttää NTLM-tiivistettä. Tällöin NTLM-tiivistettä voidaan käyttää kellonajan salaukseen ja täten henkilöllisyyden todistamisessa KDC-palvelimelle. (Pilkington 2014.)

Hyökkääjä siis todentuu nyt esimerkkiverkossa Kerberos-protokollan avulla ”Helppari” -käyttäjätunnuksella. Seuraavaksi hyökkääjä voi käyttää apuna sovelluksia, jotka mahdollistavat ohjelmien suorittamisen etänä, kuten Windows Sysinternalsin PsExec. Kuvassa 6 esimerkkitilanteen hyökkääjä käynnistää itselleen toisen laiteen, nimeltä Admin-PC-7, komentokehotteen käyttäen IT-tuen tunnusta ja PsExec-työkalua.



KUVA 6. Esimerkki PsExecistä ja ohjelmien ajamisesta etänä

Seuraavaksi hyökkääjä voi suorittaa lateraalista liikettä verkossa kopioimalla Mimikatz-ohjelman verkon muille laitteille ja ajaa niitä etänä samalla tavoin. Toisten laitteiden muistista hyökkääjä voi etsiä NTLM-tiivisteiden lisäksi Kerberos-tikettejä, jotka itselleen kopioimalla hyökkääjä voi toteuttaa Pass-the-Ticket -hyökkäyksiä.

Mimikatzin-ohjelman kopiointi toiselle laitteelle onnistuu esimerkiksi Windowsissa valmiina olevan xcopy-komennon avulla. Alla olevalla komennolla Mimikatz kopioidaan Admin-PC-7 -laitteelle C:\temp -kansioon.

```
Xcopy mimikatz.exe \\admin-pc-7\c$\temp
```

4.2.4 Pass-the-Ticket (PtT)

PtT on hyvin samankaltainen hyökkäys kuin PtH ja se voidaan toteuttaa samoilla työkaluilla. Eroavaisuudet löytyvät siinä mitä varastetaan. PtH:ssa varastettiin kirjautuneen käyttäjän salasanan NTLM-tiiviste, PtT:ssä hyökkääjä pyrkii varastamaan käyttäjän Kerberoksen palvelutiketin tai TGT-tiketin. Palvelutiketillä hyökkääjä pääsee käsiksi vain tiettyyn resurssiin, kun taas TGT-tiketillä hyökkääjä voi pyytää lippupalvelulta pääsyä mihin vain resurssiin, johon käyttäjällä on oikeus. PtT:ssäkin varastettujen tikettien avulla tarkoituksena on esiintyä kohdeverkossa toisena henkilönä.

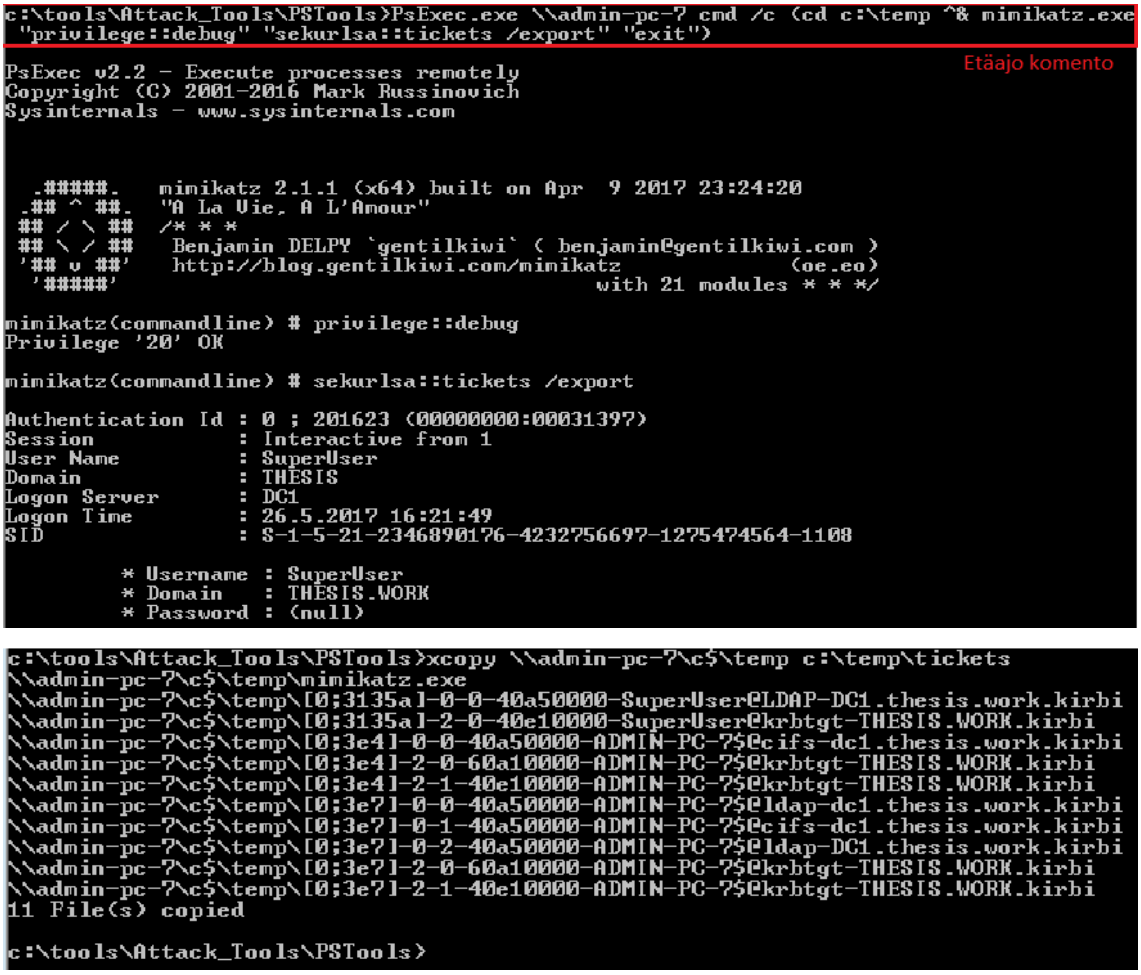
Esimerkki

Viimeksi esimerkkitilanteessa kopioitiin Mimikatz toiselle laitteelle, joten nyt se voidaan suorittaa etänä PsExec-työkalun avulla. NTLM-tiivisteiden sijaan etsitään

laitteen muistista Kerberos-tikettejä ja viedään ne C:\temp -sijaintiin kohdelaitteella. Tämä onnistuu komennolla:

```
Psexec.exe \\admin-pc-7 cmd /c (cd c:\temp ^&
mimikatz.exe "Privilege::debug" "Sekurlsa::tickets
/export")
```

Tämän jälkeen kopioidaan viedyt tiketit takaisin alkuperäisellä laitteelle C:\temp\tickets -kansioon xcopyn avulla. Kuvassa 7 on nähtävissä Mimikatzin suoritus etänä PsExecin avulla ja osa tikettien viennin tulosteesta, lisäksi toisessa ikkunassa on esitetty vietyjen tikettien kopiointi takaisin alkuperäiselle laitteelle.

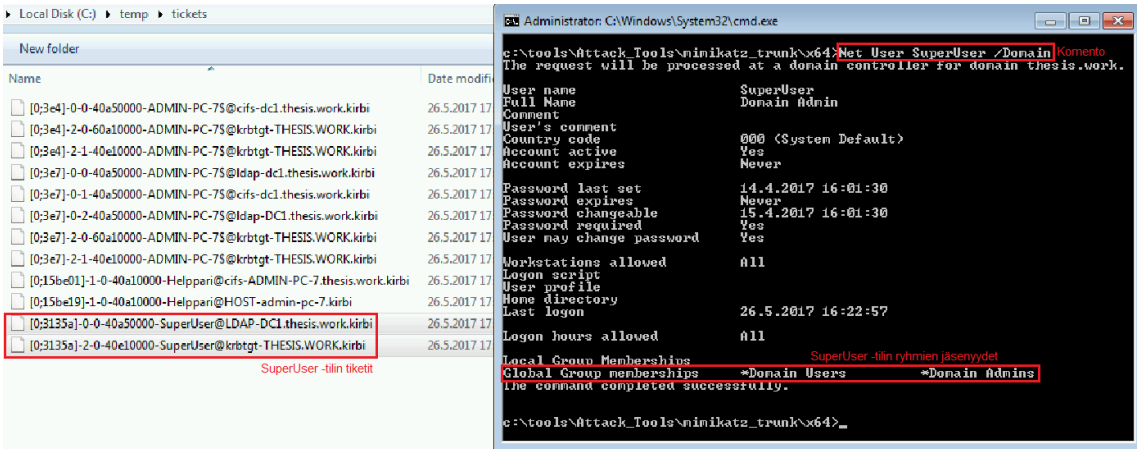


KUVA 7. Mimikatzin ajo etänä ja Kerberos-tikettien kopiointi xcopyn avulla

Kuvassa 8 näkyy C:\temp\tickets –kansio, jonka sisällä toiselta laitteelta varastetut tiketit. Tikettien joukosta löytyy myös ”SuperUser” -käyttäjätilin Kerberos-tiketit. Nimestä voi

päätellä niiden todennäköisesti olevan korkeiden käyttövaltuuksien tunnuksien tiketit, mutta asian voi myös tarkistaa komentokehotteen komennolla:

```
Net User SuperUser /Domain
```

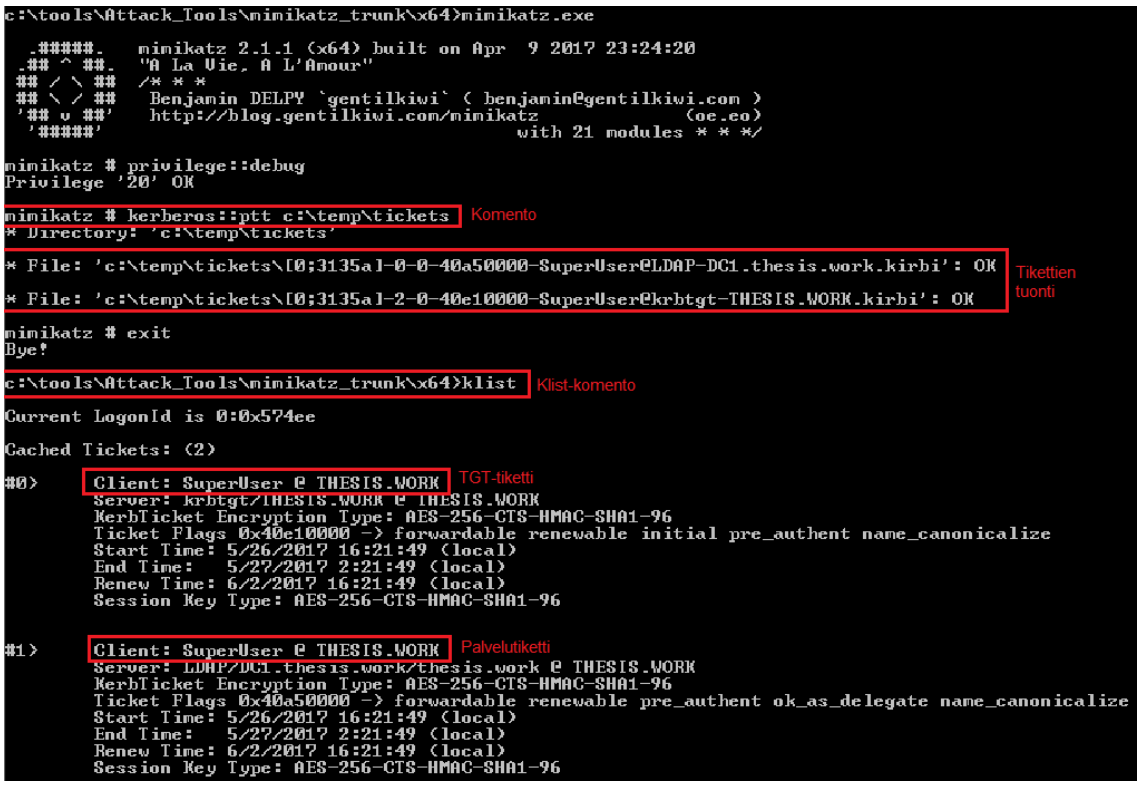


KUVA 8. Kopioidut Kerberos-tiketit ja ”SuperUser” -käyttäjätilin tiedot

PtT-hyökkäyksen toteuttamista varten kansiosta poistetaan ensin muut tiketit, lukuun ottamatta ”SuperUser” -tilin tikettejä, jonka jälkeen käskemme Mimikatzin ladata jäljelle jääneet tiketit C:\temp -kansioista komennolla:

```
Kerberos::ptt c:\temp\tickets
```

Kuvassa 9 komento on ajettu ja tämän jälkeen tarkistettu klist-komennon avulla laitteen muistissa olevat Kerberos-tiketit. Kuvasta voimme huomata, että hyökkääjä käyttää nyt "SuperUser" -tilin Kerberos-tikettejä. Tämä tarkoittaa, että hyökkääjä todentuu nyt esimerkkiverkon toimialueessa Kerberos-protokollalla ”SuperUser” -käyttäjänä ja omistaa käyttäjän oikeudet. ”SuperUser” -käyttäjä kuuluu ”Domain Admins” -ryhmään, eli hyökkääjällä on nyt hallussaan toimialueen pääkäyttäjän oikeudet ja samalla koko verkko hallussaan. Hyökkääjä voi nyt esim. luoda ja poistaa käyttäjiä tai määritellä verkon käyttäjien ja laitteiden käyttöoikeuksia.



KUVA 9. Kerberos-tikettien tuonti kansiosta Mimikatz-ohjelmalla ja klist-komento

Hyökkääjän liikkuminen verkossa voidaan kuitenkin edelleen estää, jos hänen haltuunsa saamien tunnuksien salasanat vaihdetaan tai vaarantuneet käyttäjätunnukset poistetaan toimialueesta. Hyökkääjä voi kuitenkin jatkaa hyökkäystään ja taata itselleen pysyvämmän läsnäolon kohdeverkossa. Tätä varten hyökkääjän tulee siirtyä verkon toimialuepalvelimelle, jossa hyökkääjä voi toteuttaa hyökkäyksensä seuraavan vaiheen, eli kohteessa pysyvyyden varmistamisen.

4.2.5 Skeletonkey

Skeletonkey-hyökkäys on jatkoa muille käyttäjätunnusvarkauksille. Skeletonkey-hyökkäyksessä hyökkääjä muokkaa Lsass.exen, siis ohjelman jonka vastuulla todentaminen on, ohjelmakoodia niin, että hän saa luotua takaportin kaikkiin toimialueen käyttäjätileihin. Skeletonkeyn voidaan siis sanoa olevan yleisavain, salasana joka käy kaikkiin käyttäjätileihin, käyttäjien oikean salasanan lisäksi. Tämä tekee hyökkäyksestä erityisen petollisen, koska oikeat käyttäjät pystyvät edelleen kirjautumaan omalla salasanallaan normaalisti, eivätkä voi tietää tunnustensa vaarantuneen. (Harris ym. 2017, 36.)

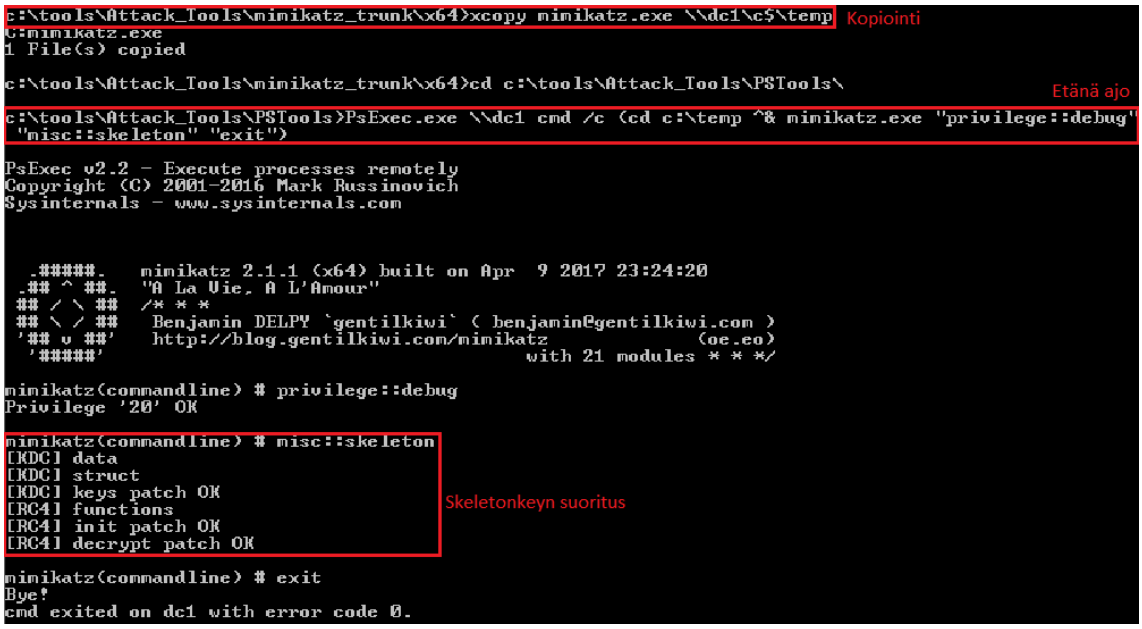
Skeletonkeyn avulla hyökkääjän on mahdollista kirjautua palveluihin tileillä, joiden odotetaankin käyttävän kyseisiä palveluita. Tällöin verkkoa valvovat ohjelmistot eivät kiinnitä hyökkääjään huomiota ja hyökkääjä voi jatkaa toimiaan verkossa pidempään huomaamattomasti. (Greiner 2015.)

Esimerkki

Myös Skeletonkey-hyökkäys on myös mahdollista toteuttaa Mimikatz-ohjelman avulla. Hyökkäyksen toteuttamista varten Mimikatz on ensin kopioitava toimialuepalvelimelle. Kopioimisen jälkeen ohjelma ajetaan etänä PsExecin avulla, jolloin Mimikatz muokkaa palvelimen Lsass.exeä luoden yleisavaimen tileihin. Kopiointi ja ohjelman ajaminen etänä onnistuvat komennoilla:

```
Xcopy mimikatz.exe \\dc1\c$\temp

Psexec.exe \\dc1 cmd /c (cd c:\temp ^& mimikatz.exe
“privilege::debug” “misc::skeleton” “exit”)
```



KUVA 10. Mimikatzin kopiointi ja Skeletonkey-hyökkäys etänä PsExecin avulla

Kuvassa 10 komennot on ajettu ja Lsass.exe muokkaus suoritettu. Mimikatz-ohjelma luo oletuksena yleisavaimeksi salasanan “mimikatz”. Tämä on kovakoodattu Mimikatz-ohjelmaan. (Harris ym. 2017, 36.) Tämän salasanan kanssa hyökkääjä voi nyt käyttää mitä tahansa verkossa käytössä olevaa kirjautumistunnusta ja kirjautua kuten normaali

käyttäjä. Tämä tarkoittaa, että hyökkääjällä on nyt olemassa takaportti jokaiseen tiliin toimialueella, eikä yhden tilin sulkeminen estä hyökkääjän liikkumista verkossa.

4.2.6 Golden Ticket

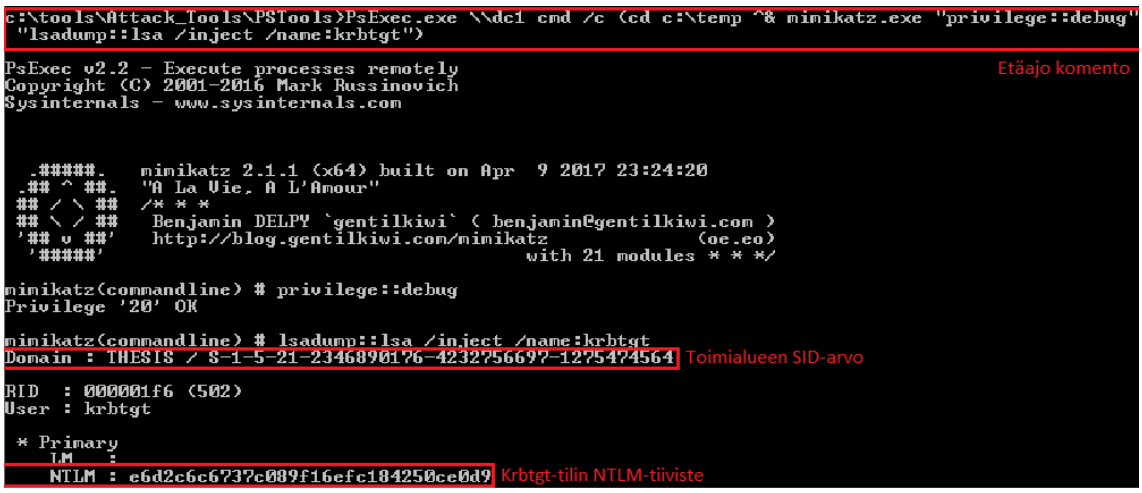
Toinen hyökkäys jonka avulla hyökkääjä voi saavuttaa pysyvyyttä kohdeverkossa on Golden Ticket -hyökkäys. Golden Ticket -hyökkäyksessä hyökkääjä luo itse Kerberoksen TGT-tiketin, jonka voimassaoloaika on 10 vuotta. Hyökkääjä voi luoda TGT-tiketin mille tahansa käyttäjälle, jolloin hän voi pyytää myös mille tahansa käyttäjälle palvelutikettejä mihin tahansa palveluun. (O´Leary 2015, 380.) Tämän vuoksi tietoturva-asiantuntija Roger A. Grimesin mukaan Golden Ticket ei ole vain väärennetty Kerberos-tiketti, se on ennemminkin väärennetty KDC-palvelin (Grimes 2014).

Kerberoksen TGT-tiketti on todellisuudessa ainoastaan palvelutiketti palveluun nimeltä krbtgt, joka pyörii kaikilla KDC-palvelimilla. Palvelun salasana on joka paikassa sama ja tällöin myös sen salasanan tiiviste on sama. Usein salasana on myös yhtä vanha kuin käytössä oleva toimialue, koska harva ylläpitäjä on sitä koskaan vaihtanut. Krbtgt-tilin salasanaa käytetään Kerberos-todennuksessa KDC-palvelimella TGT-tikettien salaamiseen asiakaan ja palvelimen välillä. Itseluotujen TGT-tikettien käyttö voidaan estää vaihtamalla krbtgt-tilin salasana kahdesti, tämä nollaa tilin ja kaikki luodut tiketit.

Esimerkki

Jotta hyökkääjä voi luoda itselleen TGT-tiketin, täytyy hyökkääjällä olla jo verkossa pääkäyttäjän oikeudet ja pääsy toimialuepalvelimelle. Lisäksi hyökkääjän täytyy saada haltuunsa krbtg-tilin salasanan NTLM-tiiviste tai AES-avain ja toimialueen SID-arvo (Security Identifier). Kaikki tarvittavat tiedot ovat saatavilla Mimikatzin avulla. Esimerkkihyökkääjällä on jo toimialueen pääkäyttäjän oikeudet hallussaan, jolloin hän voisi vain kirjautua toimialuepalvelimelle ja suorittaa Mimikatzin siellä, mutta kuvassa 11 ohjelma kuitenkin suoritetaan etänä Victim-PC-7:lta PsExecin avulla komennolla:

```
"Psexec.exe \\dc1 cmd /c (cd c:\temp ^& mimikatz.exe
"Privilege::debug"        "Lsadump::lsa        /inject
/name:krbtgt")
```



KUVA 11. Esimerkkiympäristön Krbtgt-tilin NTLM-tiiviste ja toimialueen SID-arvo

Kun hyökkääjä saa haltuunsa krbtgt-tilin NTLM-tiivisteen ja muut tiedot, voi hän syöttää ne Mimikatz-ohjelmaan ja luoda itselleen TGT-tiketin. Tikettiä luodessa voidaan määrittää lisäksi useita parametreja, joilla voidaan vaikuttaa luotavaan TGT-tikettiin. Alla on esimerkkikomento, jolla luodaan Golden Ticket Mimikatzillä.

```
"Privilege::debug" "Kerberos::golden
/user:administrator /domain:thesis.work
/sid:S-1-5-21-2346890176-4232756697-1275474564
/rc4:e6d2c6c6737c089f16efc184250ce0d9 /id:500
/groups:500,512,513 /ticket:luotu-TGT.kirbi"
```

Esimerkkikomennossa käytetyt parametrit on selvitetty taulukossa 5. RID-arvolla tarkoitetaan SID-arvon viimeisiä merkkejä. Käyttäjän RID:500 esimerkiksi tarkoittaa pääkäyttäjää (Administrator). Ryhmä RID:500 on ”Administrators” -ryhmä, RID:512 on ”Domain Users” -ryhmä ja RID:513 puolestaan on ”Domain Administrators” -ryhmä. (Lincoln 2014.)

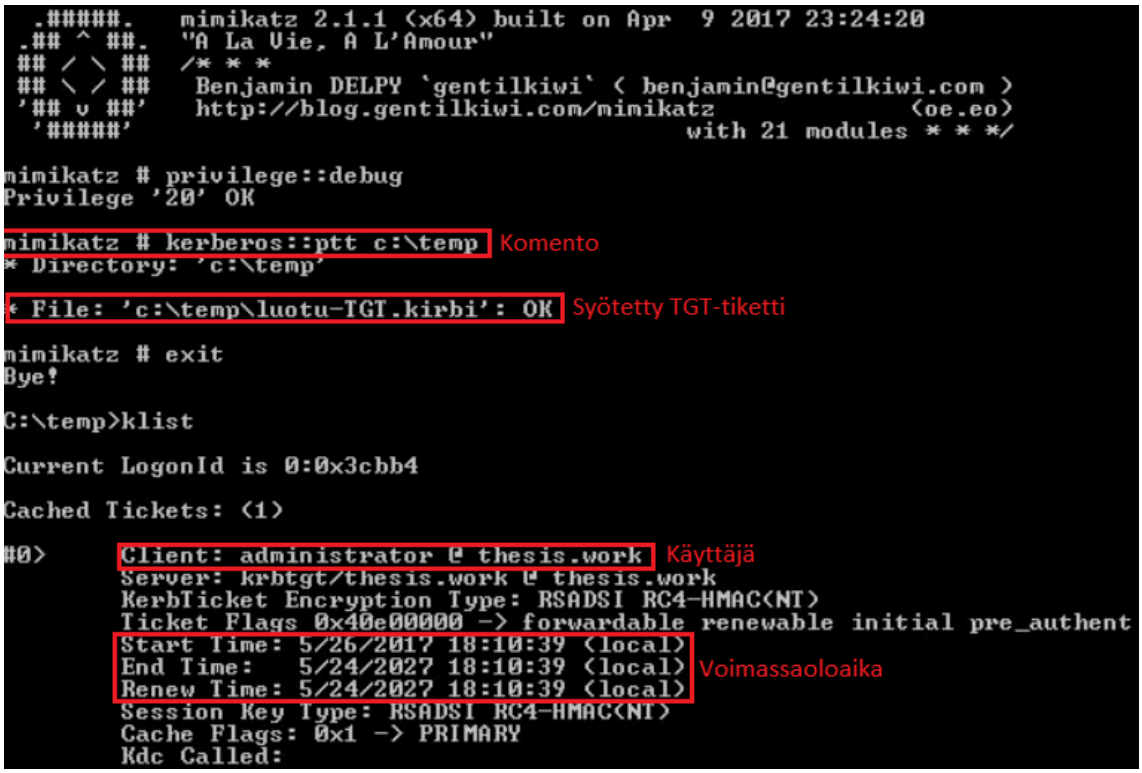
TAULUKKO 5. Golden Ticketin luomisessa käytetyt parametrit

Komento:	Selite:
/domain:thesis.work	Toimialueen nimi
/sid:S-1-5-21-2346890176-4232756697-1275474564	Toimialueen SID-arvo
/rc4:e6d2c6c6737c089f16efc184250ce0d9	Krbtgt-tilin NTLM-tiiviste
/user:administrator	Käyttäjänimi
/id:500	Käyttäjän RID-arvo
/groups:500,512,513	Ryhmien RID-arvot
/ticket:luotu-TGT.kirbi	Tiketin tiedostonimi

Kun tiketti on luotu, se voidaan syöttää Mimikatz-ohjelmalla samoin kuin muutkin Kerberos-tiketit, eli komennolla:

```
Kerberos::ptt C:\temp
```

Kuvassa 12 luotu TGT-tiketti, nimeltä ”luotu-TGT.kirbi”, on syötetty Mimikatz-ohjelmaan. Lisäksi kuvassa on suoritettu klist-komento, joka kertoo, että hyökkääjä todentuu nyt ”Administrator” -käyttäjänä ja TGT-tiketin voimassaolo aika on lähes 10 vuotta. Tiketti olisi myös mahdollista syöttää jo luodessa käyttämällä `/ptt` -parametria.



KUVA 12. Luodun TGT-tiketin syöttäminen ja klist-komento

5 KÄYTTÄJÄTIETOPOHJAINEN TIETOTURVA

5.1 Microsoft Advanced Threat Analytics

Advanced Threat Analytics on Microsoftin käyttäjien ja kohteiden käyttäytymisanalyysin perustuva paikallinen tietoturvaratkaisu. Ohjelmisto ei ole alun perin Microsoftin itse kehittämä, vaan se pohjautuu israelilaisen tietoturvayhtiön Aoraton kehittämään teknologiaan. Microsoft osti Aoraton itselleen vuonna 2014 tarkoituksenaan tarjota yritysasiakkaillensa helppokäyttöinen ja vähän ylläpitoa vaativa tietoturvaratkaisu kehittyneiden tietoturvauhkien havainnointiin. Microsoft julkaisi ohjelmiston vuonna 2015 ja se on nykyään saatavilla osana Microsoftin Enterprise Mobility + Security -tuotepakettia. (Numoto 2014; Simons 2015.)

Enterprise Mobility + Security -tuotepaketin hinnat lähtevät 8.75$/käyttäjä kuukaudessa. ATA on saatavilla myös itsenäisenä ohjelmistona, jolloin sen hinnoittelu perustuu myytyihin lisensseihin per käyttäjä ja käyttöjärjestelmä. Vähittäismyyntihinnat itsenäiselle ATA -ohjelmistolle ovat 80$/käyttäjä ja 61.50$/käyttöjärjestelmä vuodessa. Hinnat saattavat vaihdella kohdemaittain ja niihin on mahdollista saada myös erilaisia alennuksia. ATA:sta on lisäksi saatavilla 3-kuukauden ilmainen kokeilujakso. (Microsoft 2015.)

ATA:n etuihin perinteisiin tunkeutumisen havainnointi- ja estämisjärjestelmiin verrattuna kuuluvat asennuksen helppous, tehokas koneoppiminen, yhteensopivuus jo olemassa olevien SIEM-ratkaisujen (Security Information and Event Management) kanssa ja päivitykset Windows Updaten kautta. ATA:n avulla on mahdollista havaita verkossa erilaisten kehittyneiden kyberhyökkäystekniikoiden ja heikkojen protokollien käyttöä ja lisäksi ATA valvoo verkon käyttäjiä ja kohteita epäilyttävän toiminnan varalta. Esimerkkejä ATA:n havaitsemista uhkista ja riskeistä on esitelty lyhyesti taulukossa 6.

TAULUKKO 6. Esimerkkejä ATA:n verkosta havaitsemia uhkista (Microsoft 2016c)

Nimi:	Selite:
Käyttäjien epänormaali toiminta	Salasanojen jakaminen, tuntemattomat kirjautumiset, lateraalinen liike
Kehittyneet kyberhyökkäystekniikat	Pass-the-Hash, Pass-the-Ticket, Overpass-the-Hash, Golden Ticket, Brute Force, etäohjelmien suoritus, sisäinen tiedustelu
Tietoturvauhat ja riskit	Tunnetut protokolla haavoittuvuudet ja luottosuhteiden katkeamiset

ATA valvoo verkkoa lähes kaikilta hyökkäysketjun eri vaiheilta, pois lukien ulkoinen tiedustelu. Se pystyy havaitsemaan useita erilaisia sisäisen tiedustelun muotoja, kuten DNS-tiedustelu (Domain Name System Reconnaissance), käyttäjien luettelointi, yksiköiden SAMR-luettelointi (Security Account Manager Remote Protocol Enumeration), sekä SMB-istuntojen luettelointi (Server Message Block Session Enumeration). (Microsoft 2016a.)

Tärkeää on kuitenkin huomata, että ATA ainoastaan valvoo verkkoa hyökkäysten ja uhkien varalta, se ei siis estä niitä toteutumasta. Hyökkäyksen sattuessa ylläpitäjät saavat ainoastaan tiedon tapahtuneesta ja suosituksia, miten tilanteessa kannattaisi toimia.

5.1.1 Osat ja vaatimukset

Microsoft ATA -tietoturvaratkaisu koostuu kahdesta tai kolmesta osasta riippuen valitusta asennustavasta. Nämä osat ovat ATA Center, ATA Gateway ja ATA Lightweight Gateway. Näistä ATA Gateway ja ATA Lightweight Gateway ovat käytännössä sama asia, mutta Lightweight Gateway on tarkoitettu suoraan toimialuepalvelimelle asennettavaksi ja Gateway puolestaan omaksi erilliseksi palvelimekseen. Myös molempien yhtäaikainen käyttö on mahdollista, jos ympäristössä on käytössä useampia toimialuepalvelimia. ATA:n kaikki osat on myös mahdollista asentaa joko fyysiselle tai virtuaaliselle palvelimelle. (Diogens, Gilbert & Mazzoli 2016, 86.)

ATA Center on tietoturvaratkaisun keskus, jolle Gatewayt lähettävät käsittelemänsä datan. Center rakentaa saamastaan datasta ohjelmiston käyttämän MongoDB-tietokannan. Lisäksi Center pyörittää myös ATA:n hallintakonsolia ja ajaa hyökkäystekniikat ja epäilyttävän toiminnan havaitsevia algoritmeja. (Diogens ym. 2016, 86.)

ATA Gateway on tietoturvaratkaisun portti, jolle peilataan kaikki verkkoliikenne, joka kulkee toimialuepalvelimelle tai toimialuepalvelimelta. Tämän lisäksi Gatewaylle voidaan ohjata olemassa olevien SIEM-ratkaisujen tai Syslog-palvelimien liikennettä. Jos tällaisia ratkaisuja ei ole käytössä, voidaan Gatewaylle ohjata myös Windowsin tapahtumalokin kirjautumiseen liittyvät viestit (ID 4776). Gateway jäsentelee saamansa datan ja ohjaa sen edelleen Centerille. Yhden Gateway-palvelimen on mahdollista valvoa useita toimialuepalvelimia, kunhan palvelimien yhteenlasketut pakettimäärät sekunnissa pysyvät alle 50 000 kappaleen. (Microsoft 2016a.)

ATA Lightweight Gateway on kevyempi vaihtoehto normaalille Gatewaylle. Se voidaan asentaa suoraan verkon toimialuepalvelimelle, jolloin erillistä palvelinta tai portin peilaus konfiguraatiota ei tarvitse toteuttaa. Lightweight Gatewayn käytölle on kuitenkin rajoituksensa, sillä sitä voidaan käyttää vain, jos palvelimen yhteenlaskettu pakettimäärä sekunnissa ei ylitä 10 000 kappaletta. Microsoft suosittelee kevyemmän version käyttöä esimerkiksi haarakonttoreissa, joissa liikenne on vähäisempää. (Microsoft 2016a.)

ATA:n palvelimien laitteistovaatimukset riippuvat asennettavan verkon liikenteen määrästä. Microsoft tarjoaa ilmaisen työkalun nimeltä ATA Sizing Tool, jonka avulla verkon pakettimäärän voidaan selvittää helposti. Toinen vaihtoehto on mitata pakettimäärä itse käyttämällä Windows-käyttöjärjestelmistä löytyvää Performance Monitor -työkalua. Performance Monitoria käytettäessä mitataan toimialuepalvelimen tietoliikenneportin pakettimäärä sekunnissa 24-tunnin ajan. Kummalla tavalla tahansa toteutettuna mittaus kannattaa suorittaa useampaan kertaan ja eri viikon aikoina. Tällöin pakettimäärien keskiarvo saadaan mitattua mahdollisimman luotettavasti ja siten laitteiston vaatimukset suunniteltua riittävän tarkasti. (Microsoft 2016a.)

Käyttöjärjestelmäksi ATA:n osat vaativat Windows Server 2012 R2 tai Server 2016. ATA:n palvelimien ei ole välttämätöntä olla toimialueen jäseniä vaan palvelimet voidaan pitää myös erillisenä työryhmänä. Tällöin hyökkääjän on vaikeampi havaita ATA:n

olemassaoloa verkossa, mutta samalla se lisää ylläpidon työtä, koska tällöin esim. keskitetty laitteiden päivitys ei ole mahdollista. ATA:n toiminta vaatii myös, että verkon toimialuepalvelin on Windows Server 2008 tai uudempi ja että sille on määritetty toimialueeseen oma käyttäjätili. Käyttäjätilille riittävät lukuoikeudet toimialueella ja sitä käytetään vain ATA:n yhdistämiseksi toimialueeseen. (Diogens ym. 2016, 92.)

5.1.2 Toimintaperiaate

Microsoft ATA käyttää hyväkseen koneoppimisalgoritmeja oppiakseen verkon kohteiden ja käyttäjien normaalin käyttäytymisen ja näiden suhteet toisiinsa. Tämä tapahtuu tietoliikennepakettien syvätarkastuksen avulla, eli käytännössä ohjelma tutkii jokaisen paketin jokaisen bitin, joka sille ohjataan. (Diogens ym. 2016, 84.)

Koneoppimisen ansiosta ohjelmistolle ei tarvitse erikseen luoda sääntöjä tai lähtötasoja. Ohjelmisto vaatii kuitenkin aluksi vähintään 3-4 viikon seuranta-ajan, jonka aikana se oppii itsenäisesti verkon kohteiden ja käyttäjien normaalin käytöksen. Tämän seuranta-ajan jälkeenkin ohjelmisto jatkaa oppimista ja mitä pidempään se verkossa on käytössä, sen tarkemmin se oppii verkon kohteet ja käyttäjät tuntemaan. Hyökkäystekniikat ja heikkoudet protokollissa ATA pystyy kuitenkin havaitsemaan heti asennuksen jälkeen, koska ne pohjautuvat jo tiedossa oleviin heikkouksiin ja hyökkäyskuvioihin (Diogens ym. 2016, 87.)

Käytösanalyyseihin perustuva valvonta voidaan selittää helpoiten luottokorttiyhtiö -esimerkin avulla. Luottokorttiyhtiöt seuraavat missä yhtiön myöntämiä luottokortteja käytetään. Jos yhtiö havaitsee korttia käytetyn oudossa paikassa, kuten esimerkiksi vieraassa maassa, herättää se epäilyksen luottokorttiyhtiössä. Tällöin se voi ottaa yhteyttä kortin omistajaan ja kysyä onko tämä käyttänyt korttiaan esim. matkoilla ollessaan, vai käytetäänkö korttia mahdollisesti väärin. Microsoft ATA tuo saman periaatteen tietoturvaan, luottokortin käytön sijaan se voi valvoa mihin palveluihin käyttäjä kirjautuu, milloin ja millä laitteella. Microsoft jakaa ATA:n toiminnanvaiheet 4-osaan. Nämä 4-vaihetta selityksineen on listattu alla taulukossa 7.

TAULUKKO 7. ATA:n toiminnanvaiheet (Diogens ym. 2016, 86)

Vaihe:	Selite:
Analysointivaihe	ATA tutkii verkon liikennettä.
Oppimisvaihe	ATA profiloi käyttäjien, laitteiden ja resurssien normaalin toiminnan. Tämän profiloinnin pohjalta se luo organisaation turvallisuuskaavio, joka osoittaa profiloitujen kohteiden suhteet toisiinsa.
Havainnointivaihe	ATA etsii poikkeamia normaalista toiminnasta.
Hälytysvaihe	ATA hälyttää havaitsemastaan poikkeamasta. Hälytyksen lisäksi ATA tarjoaa myös toimintaohjeita ja suosituksia, miten tilanteessa kannattaa edetä.

5.2 Asennusympäristö

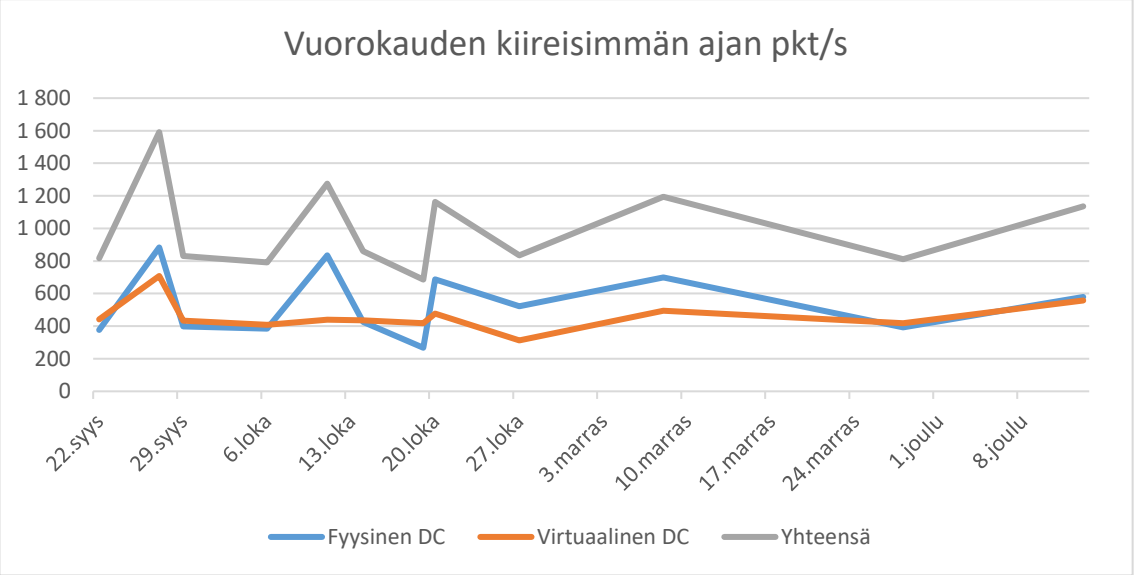
Asensin Microsoftin Advanced Threat Analytics -ohjelmiston Tampereen ammattikorkeakoulun tietojenkäsittelyn harjoitus- ja laboratorioverkko WPK:hon, joka on kahden Windows Server 2012 R2 toimialuepalvelimen verkkoympäristö. Toimialuepalvelimista toinen on virtuaalinen ja toinen fyysinen. Verkko koostuu näiden ja muiden palvelimien lisäksi myös noin 120:sta työasemasta jotka käyttävät Windows 7, Windows 8.1 ja Windows 10 -käyttöjärjestelmiä. Verkon käyttäjinä ovat kaikki tietojenkäsittelyn opiskelijat ja opettajat. Verkossa jokaisella käyttäjällä on paikallisen pääkäyttäjän oikeudet kirjaudutulle laitteelle.

Asennus aloitettiin verkon pakettimäärien selvittämisellä. Pakettimäärien mittaamiseen käytettiin Microsoftin tarjoamaa ilmaista ja helppokäyttöistä ATA Sizing Toolia, jolla pakettimäärät mitattiin useaan otteeseen syksy-talvi 2016 välillä. Mittauksissa havaittiin muutamaan otteeseen huomattavan suuria heittoja keskiarvoon nähden. Kiireisimpänä aikana pakettimäärät olivat yli 27 000 pkt/s, ollen kuitenkin useimmiten vain noin 1000 pkt/s. Vuorokauden keskiarvon ollessa yleensä alle 500 pkt/s.

Pakettimäärien mittauksessa havaittiin, että pakettimäärät toimialuepalvelimilla olivat pääsääntöisesti selvästi alle 10 000 pkt/s, joten myös kevyemmän Lightweigth Gatewayn käyttäminen olisi mahdollista. Päädyin kuitenkin asentamaan ympäristöön molemmat

Gatewayt, normaalin Gatewayn keräämään dataa fyysiseltä toimialuepalvelimelta ja Lightweight Gatewayn keräämään dataa virtuaaliselta toimialuepalvelimelta.

Kuviossa 10. on esitetty mittaustulokset, joista on poistettu yksi noin 15 000 pkt/s ja yksi yli 27 000 pkt/s mittaustulos. Tulokset poistettiin, jotta kuvio selventäisi tarkemmin verkon keskimääräisiä kiireisenajan pakettimääriä toimialuepalvelimilla. Huomattavaa on, että taulukko ilmoittaa vuorokauden kiireisimmän ajan pakettimäärän sekunnissa, ei pakettimäärien keskiarvoa vuorokaudessa.



KUVIO 10. WPK-verkon pakettimäärät (pkt/s) vuorokauden kiireisimpänä aikana

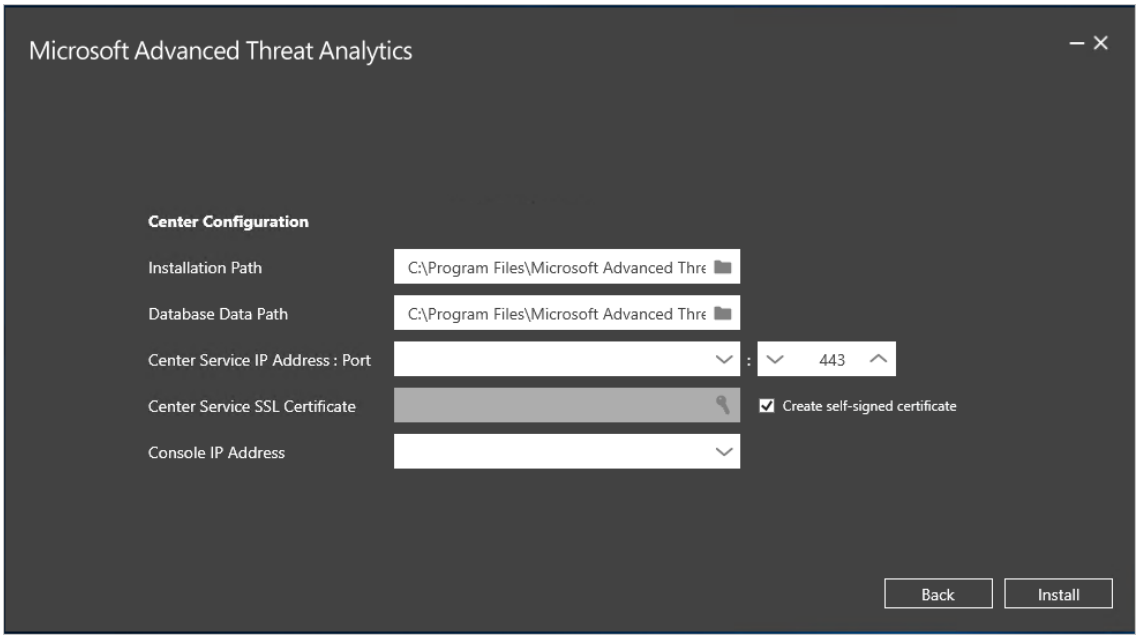
Taulukon avulla saatiin pidemmän aikavälin katsaus pakettimääristä, joka mahdollisti laitteistovaatimuksien tarkan suunnittelun. Laitteistovaatimukset mitoitettiin kuitenkin hieman yläkanttiin, jättäen varaa myös liikenteen kasvamiselle tulevaisuudessa. Mittausten aikana havaittiin myös, että virtuaalisen toimialuepalvelimen prosessoriytimien määrä oli liian vähäinen, joka johti kiireisimpänä aikana virtuaalipalvelimen ylikuormittumiseen. Koska palvelimelle asennettava Lightweight Gateway tulisi kuormittamaan palvelinta entisestään, lisättiin sille prosessoriytimiä jo ennen asennuksen aloittamista. Palvelimen ollessa virtuaalinen, oli lisääminen helppo toteuttaa. Ennen asennuksen aloittamista toimialueelle luotiin vielä ATA:n vaatima käyttäjätili, jolle annettiin luku-oikeudet toimialueelle.

5.2.1 ATA Center

ATA Centeriä varten luotiin uusi virtuaalipalvelin jo olemassa olevalle fyysiselle palvelimelle. Käyttöjärjestelmäksi valittiin Windows Server 2016, johon ennen asennuksen aloittamista päivitettiin kaikki saatavilla olevat päivitykset. Uusi virtuaalipalvelin nostettiin myös toimialueen jäseneksi, jotta ylläpito olisi helpompi hoitaa tulevaisuudessa.

ATA Center vaatii kaksi erillistä IP-osoitetta, joista toista käytetään hallintakonsolin osoitteena ja toista yhteysosoitteena Gateway-palvelimille. Molemmat IP-osoitteet lisättiin yhdelle ja samalle verkkoadapterille.

Asennettava ATA:n versio oli 1.7 ja sen asennus oli varsin suoraviivainen, koska palvelimeksi valittiin Windows Server 2016 johon erillisiä asennettavia esivaatimuksia ei ollut. Asennusohjelmassa valittiin asennuspolku ja tietokannan tallennuspolku, sekä käytettävä sertifikaatti ja mitä IP-osoitetta hallintakonsolin haluttiin käyttävän. Käytin asennuksessa oletustallennuspolkuja ja itse-allekirjoitettua sertifikaattia, mutta sertifikaatti on myöhemmin halutessa mahdollista korvata myös ulkoisella sertifikaatilla. Kuvassa 13 on esitetty ATA:n asennusohjelman asetukset.



KUVA 13. ATA Centerin asennusohjelma (Microsoft 2016a)

Valintojen jälkeen asennusohjelma asentaa ATA Centerin osat joihin, kuuluvat ATA Center -palvelu, MongoDB-tietokanta, IIS-palvelu (Internet Information Service), itse-allekirjoitettu sertifikaatti ja Performance Monitorille tehty tiedonkeruutyökalujen sarja.

Asennuksen jälkeen ohjelmaan kirjaudutaan sisään työpöydän Microsoft ATA Console -pikakuvakkeesta samalla tunnuksella, kuin millä ohjelmisto asennettiin. Heti kirjautumisen jälkeen ATA Center pyytää käyttäjätunnusta, salasanaa ja toimialueen nimeä. Tähän syötetään aiemmin luodun, lukuoikeuksilla varustetun käyttäjätilin kirjautumistiedot. Tämän jälkeen Centeriltä voi ladata ATA Gatewayn asennuspaketin.

Gatewayn asennuspaketti on pakattu zip-tiedosto, joka sisältää kaikki tarvittavat asennusohjelman asetukset, joiden avulla ATA Gateway saa automaattisesti yhteyden ATA Centerille. Samaa asennuspakettia käytetään, sekä normaalin että kevyemmän Lightweight Gatewayn asentamiseen. Asennusohjelma osaa tunnistaa yritetäänkö sitä asentaa toimialuepalvelimelle vai tavalliselle palvelimelle, jolloin se tarjoaa vaihtoehdot asennuspaikan mukaan.

5.2.2 ATA Gateway

ATA Gatewaytä varten luotiin myös uusi virtuaalipalvelin samalle fyysiselle palvelimelle kuin ATA Center. Myös Gatewayn käyttöjärjestelmäksi valittiin Windows Server 2016, johon päivitettiin aluksi kaikki saatavilla olevat päivitykset ja myös se nostettiin toimialueen jäseneksi.

Gateway tarvitsee toimiakseen kaksi erillistä verkkoadapteria ja kaksi IP-osoitetta. Nämä luotiin virtuaalikoneelle ja ensimmäinen niistä osoitettiin samaan virtuaalikytkimeen kuin ATA Center ja muu sisäverkko. Toiselle adapterille luotiin uusi ulkoinen virtuaalikytkin, joka nimettiin ATA:ksi ja se yhdistettiin fyysisellä palvelimella sille erikseen omistettuun tietoliikenneporttiin.

Ennen Gatewayn asennuksen aloittamista konfiguroitiin vielä portin peilaus fyysiseltä toimialuepalvelimelta virtuaaliselle Gateway-palvelimelle. Tämä toteutettiin kahdessa vaiheessa, jossa ensin suoritettiin portin peilaus fyysiseltä toimialuepalvelimelta toiselle fyysiselle palvelimelle ja toisessa vaiheessa fyysiseltä palvelimelta virtuaaliselle

Gateway-palvelimelle. Fyysisten palvelimien välissä oli käytössä Ciscon L3-kytkin, johon ensimmäisen vaiheen portin peilaus toteutettiin komennoilla:

```
Monitor session 1 source interface G0/1 both
Monitor session 1 destination interface G0/3
```

Komento toteuttaa yksinkertaisen SPAN-monitoroinnin (Switched Port Analyzer), jossa kaikki lähdeporttiin (source) osoitettu tai sieltä tuleva liikenne kopioidaan kohdeporttiin (destination). Tässä tapauksessa kaikki fyysisen toimialuepalvelimen tuleva ja lähtevä liikenne kopioitiin kytkimen porttiin, josta yhteys meni palvelimelle, jossa virtuaalinen Gateway-palvelin tuli sijaitsemaan.

Toisessa vaiheessa kopioituva liikenne tuli saada fyysiseltä palvelimelta virtuaaliselle Gateway-palvelimelle. Tähän tarkoitukseen käytettiin Gateway-palvelimelle luotua toista verkkoadapteria, joka oli kytketty aiemmin luotuun ulkoiseen ATA-virtuaalikytkimeen. Adapterin lisäasetuksista Hyper-V Managerissa asetettiin adapterin Port Mirroring -modeksi ”Destination”.

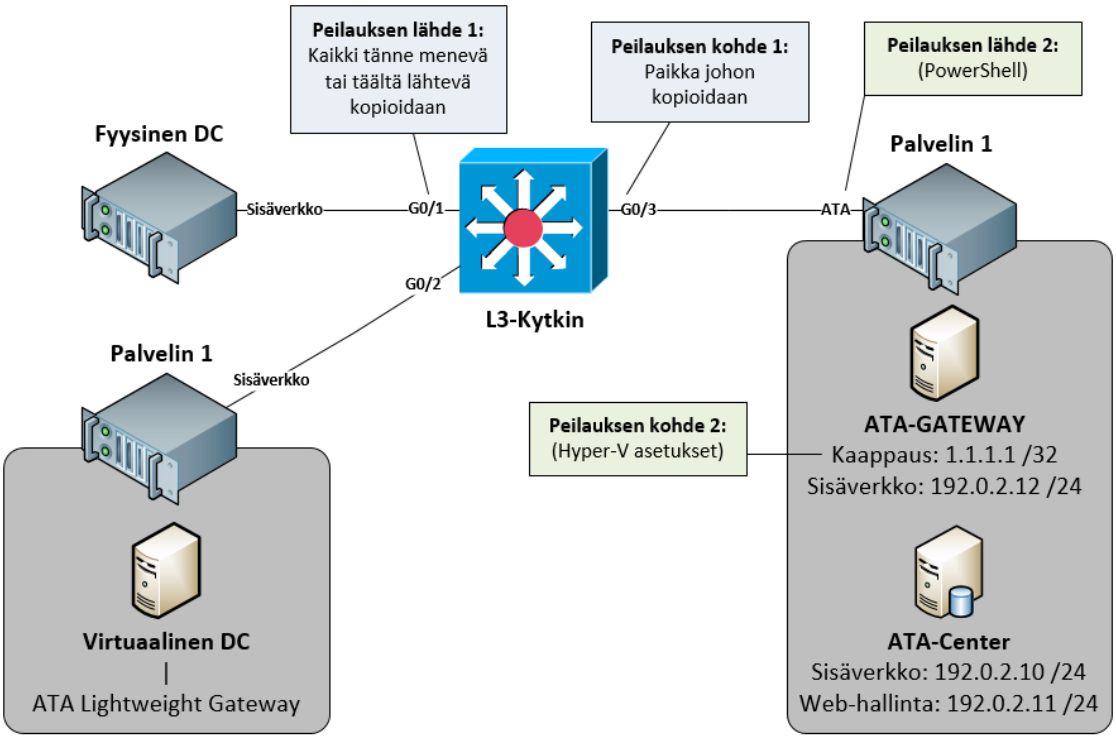
Jos myös toimialuepalvelin olisi ollut virtuaalinen, olisi portin peilaus voitu toteuttaa virtuaalikoneelta toiselle valitsemalla puolestaan toimialuepalvelimen adapterin Port Mirroring -modeksi ”Source”. Näin ei kuitenkaan tässä tapauksessa ollut, joten fyysisellä pohjapalvelimella piti ajaa PowerShell-komento, joka määritti ulkoisen verkkoliitännän virtuaalikytkimen portin peilauksen lähdeportiksi. Käytetty PowerShell-komento ja peilaus vaihtoehdot on esitetty kuvassa 14.

```
PS C:\> $ExtPort = Get-VMSystemSwitchExtensionPortFeature -FeatureId 776e0ba7-94a1-41c8-8f28-951f524251b5
# None = 0, Destination = 1, Source = 2
$ExtPort.SettingData.MonitorMode = 2
add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName "ATA" -VMSwitchExtensionFeature $ExtPort
```

KUVA 14. Fyysisen verkkoadapterin lisääminen peilauksen lähteeksi virtuaalikoneelle

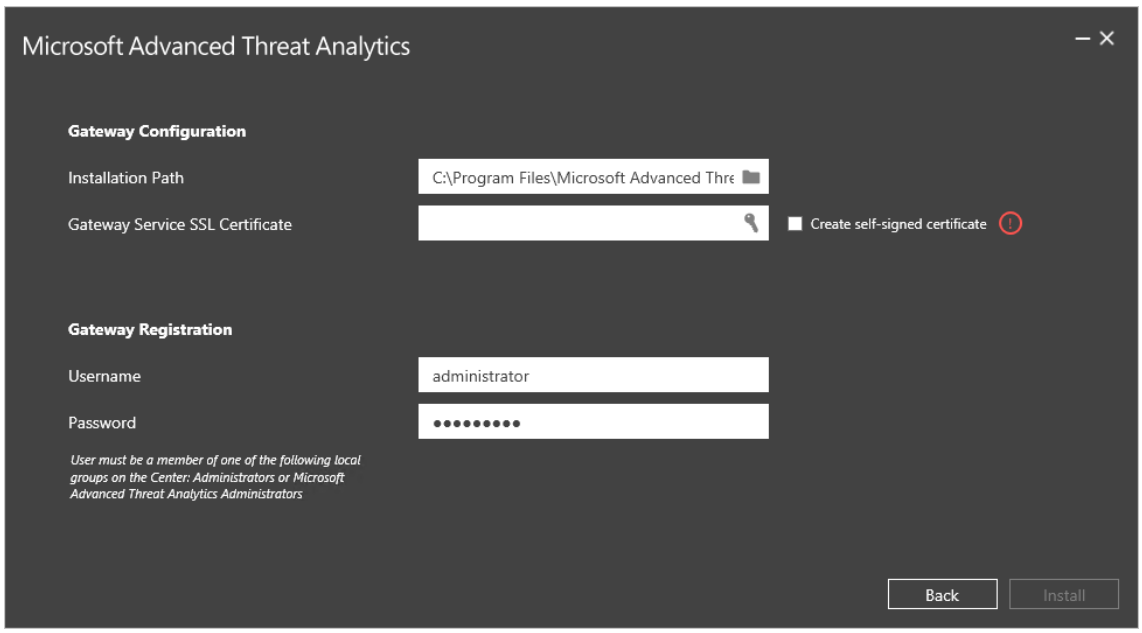
Komennon avulla portin peilaus saatiin valmiiksi eli fyysisen toimialuepalvelimen liikenne peilautumaan virtuaaliselle Gateway-palvelimelle. Liikenteen kopioituminen varmistettiin vielä Microsoftin Network Monitor -ohjelmiston avulla kaappaamalla Gateway-palvelimella Kerberos-liikennettä ja tarkkailemalla kopioituuko liikennettä palvelimelle. Liikenne kopioitui oikein, joten seuraavaksi palvelimelle siirrettiin aiemmin Centerin hallintapaneelista ladattu ATA Gatewayn asennuspaketti.

Kuviossa 11 on esitetty asennusympäristö yksinkertaistettuna ilman verkon muita osia, sekä kaksi erillistä portin peilausta lähteineen ja kohteineen. Lisäksi kuvaan on merkitty virtuaalisten Gateway- ja Center-palvelimien IP-osoitteet.



KUVIO 11. Asennusympäristön ja portin peilausten topologia

Itse Gateway-palvelimen asennus oli yhtä suoraviivainen kuin Center-palvelimenkin. Aluksi asennusohjelma tarkistaa, että laite täyttää minimi laitteistovaatimukset. Tämän jälkeen valitaan haluttu asennuspolku ja käytettävä sertifikaatti tai luodaan itse-allekirjoitettu sertifikaatti. Tämän lisäksi syötetään käyttäjätunnus ja salasana, joiden täytyy olla joko ”Administrators” tai ”Microsoft Advanced Threat Analytics Administrators” -ryhmän jäsenen. Gateway-palvelimen asennusohjelman asetukset on esitetty kuvassa 15.



KUVA 15. ATA Gatewayn asennusohjelma (Microsoft 2016a)

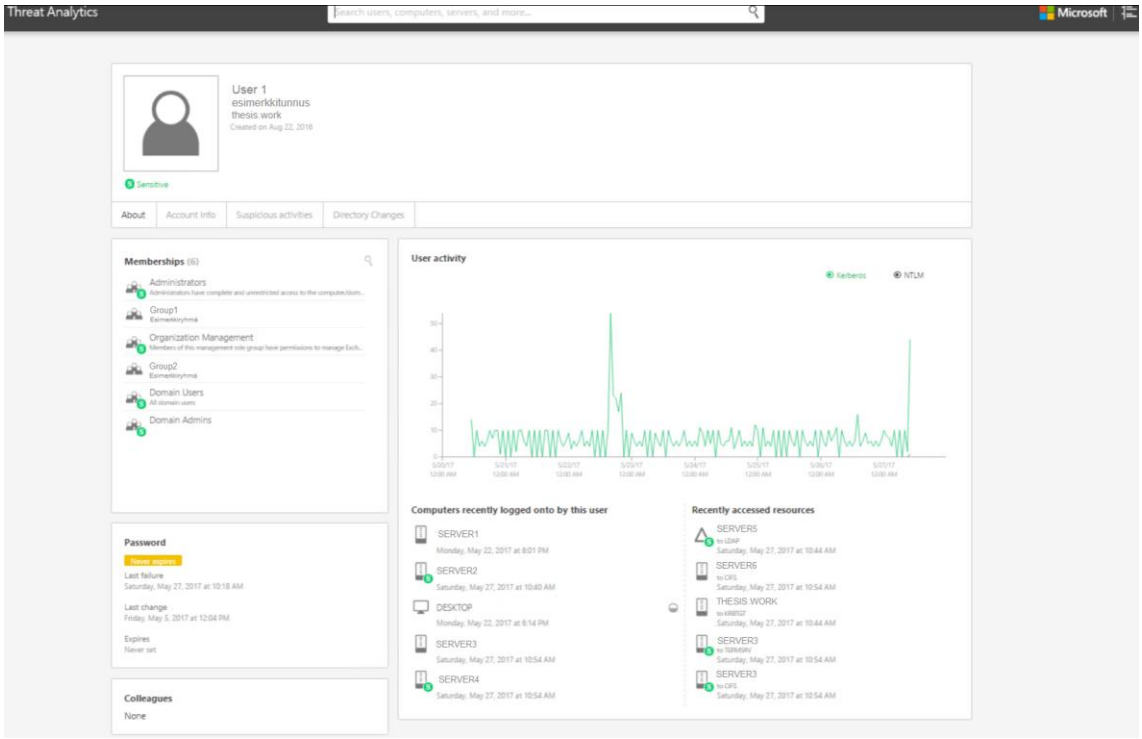
Käytin myös Gatewayn asennuksessa oletusasetuksia ja itse-allekirjoitettua sertifikaattia. Asetusten valitsemisen jälkeen asennusohjelma asentaa palvelimelle ATA Gateway -palvelun, Performance Monitorille tehdyn tiedonkeruutyökalujen sarjan ja lisäksi Microsoft Visual C++ 2013 -ohjelmistoalustan. Asennuksen jälkeen Gateway käynnistetään ja sille konfiguroidaan mitä toimialuepalvelinta sille ollaan peilaamassa ja mitä verkkoadapteria peilauksessa käytetään, lisäksi palvelin on uudelleenkäynnistettävä.

5.2.3 ATA Lightweight Gateway

ATA Gatewayn kevyempi versio asennettiin suoraan jo olemassa olevalle virtuaaliselle toimialuepalvelimelle, jonka käyttöjärjestelmänä toimi Windows Server 2012 R2. Asennukseen käytettiin samaa, aiemmin ATA Centeriltä ladattua asennuspakettia. Kevyemmän version asennus oli kaikista yksinkertaisin toteuttaa, koska edes erillistä portin peilausta ei tarvinnut konfiguroida lainkaan. Lightweight Gateway asentuu roolin tavoin palvelimelle ja se osaa kerätä ja ohjata datan Centerille suoraan ilman erillistä konfiguraatiota. Gatewayn asentumisen voi varmistaa tarkistamalla, että Microsoft Advanced Threat Analytics Gateway -palvelu pyörii laitteella.

5.3 Käyttöliittymä

ATA:n käyttöliittymä on suunniteltu yksinkertaiseksi ja informatiiviseksi. Se muistuttaa sosiaalisen median käyttöliittymiä, jossa pääikkunassa on aikajana, johon tapahtumat listataan aikajärjestyksessä. Käyttöliittymästä löytyy lisäksi hakukenttä, jonka avulla voidaan hakea käyttäjiä ja laitteita toimialueesta. Käyttäjillä ja laitteilla on oma sivunsa, josta voidaan seurata käyttäjien kirjautumisaktiivisuutta eri protokollilla ja lisäksi nähdä muita tietoja, kuten esimerkiksi vanheneeko tilin salasana tai koska se on vaihdettu. Esimerkki käyttäjäsivusta ja käyttöliittymän ulkoasusta on esitetty kuvassa 16.

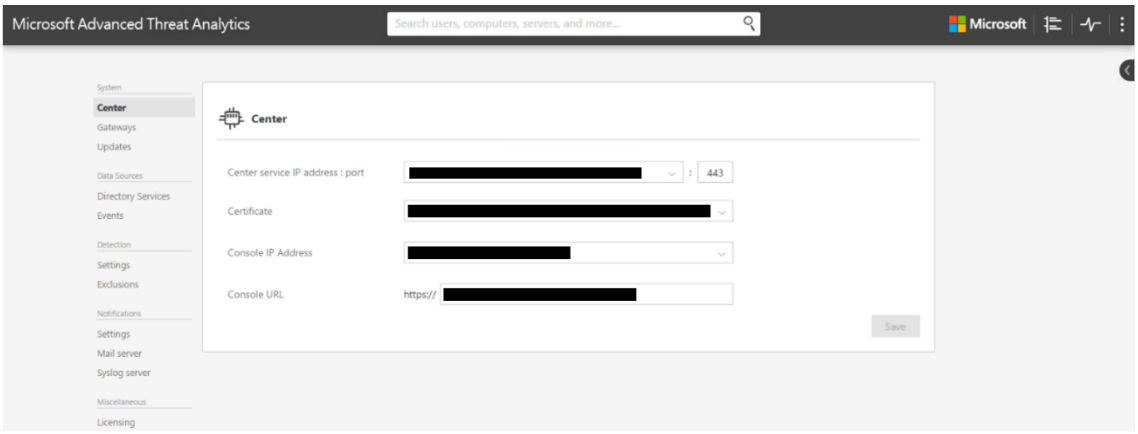


KUVA 16. Esimerkki ATA:n käyttäjäsivusta

Käyttöliittymän vasemmasta reunasta löytyy jaotellut osiot ilmoituksille eri vakavuusasteiden mukaan. Lisäksi sieltä löytyy omat osionsa avoimille, käsitellyille ja hylätyille ilmoituksille. Oikeasta reunasta puolestaan löytyy tuoreimmat hälytykset ja ilmoitukset esimerkiksi siitä, jos Center-palvelin lakkaa saamasta tietoliikennettä Gatewayltä itselleen.

Asetukset-välilehti löytyy käyttöliittymän oikeasta yläkulmasta, kolmeen päällekkäisen pisteen alta. Se tarjoaa ratkaisun kaikki asetukset yhdessä paikassa. Asetuksista voi tarkastella esimerkiksi Center- ja Gateway-palvelimien päivitysten tilannetta ja säätää

Gateway-palvelimien uudelleenkäynnistyksen manuaaliseksi tai automaattiseksi. Lisäksi asetuksista voi poissulkea IP-osoitteita, kuten esim. osoitteita joita jaetaan langattomassa verkossa DHCP:llä (Dynamic Host Configuration Protocol). Tällaisilla osoitteilla on usein lyhyt Lease-aika, jolloin ne saattavat aiheuttaa turhia DNS-tiedusteluhälytyksiä ATA:ssa. Kuvassa 17 on esitetty ATA:n hallintapaneelin asetukset-välilehti yksityiskohdat piilotettuna.



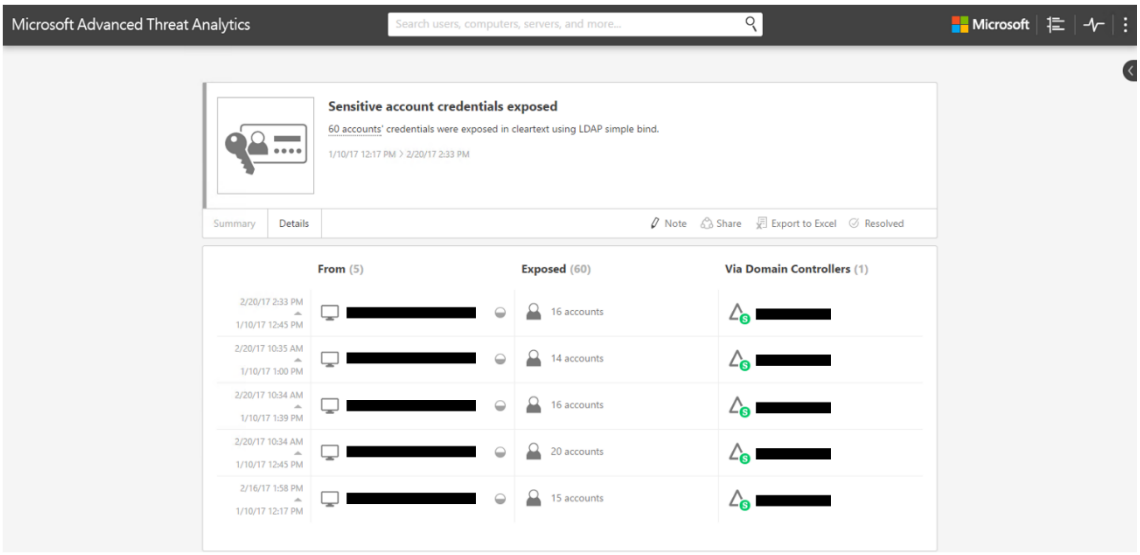
KUVA 17. Ohjelman hallintapaneelin asetukset-välilehti

Asetukset valikossa on myös mahdollista määrittää ATA lähettämään sähköposti-ilmoituksia uusista hälytyksistä, sekä halutessa lisätä Syslog- tai SIEM-palvelin ATA:n tietolähteeksi. WPK-verkossa ei kuitenkaan erillistä SIEM- tai Syslog-palvelinta ollut käytössä, joten niitä ei asennukseen konfiguroitu. Sen sijaan toimialueelle luotiin Honeytoken-käyttäjä eli ns. houkutus-tunnus jolla tehdyt kirjautumisyritykset aiheuttavat välittömästi hälytyksen ATA:ssa. Houkutus-tunnuksen lisääminen tapahtui yksinkertaisesti lisäämällä asetukset-välilehdelle halutun käyttäjän SID-arvo Honeytoken-listalle. Tällaisia houkutin-tunnuksia voi verkkoon lisätä halutessaan useampiakin. Suositeltavia houkutin-tunnuksia ovat esim. Windowsista oletuksena löytyvät ”Administrator” -tunnukset.

SIEM-palvelimen puuttuessa asetuksista otettiin asetukset-välilehden Events-valikosta käyttöön ”Windows Event Forwarding”, eli Windowsin tapahtumien edelleen lähetys. Tämän jälkeen molemmille toimialuepalvelimille konfiguroitiin Windows Event Viewer tilaus, jossa viestit ID:llä 4776 määritettiin edelleen lähetettäväksi ATA-Centerille. Tämän ansiosta ATA pystyy paremmin tarkkailemaan kirjautumisia ja niiden yrityksiä verkossa.

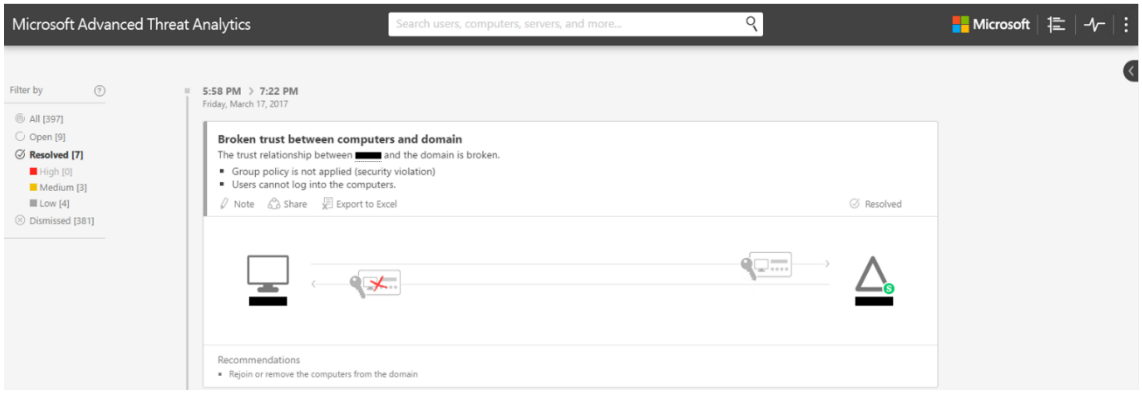
5.4 Havaintoja seuranta-aikana

Asennuksen jälkeen ATA jätettiin tarkkailemaan verkkoa, kokonaisseuranta-ajan ollessa noin 3-kuukautta. Tänä aikana ATA antoi muutamia hälytyksiä, joista ensimmäisen heti pian asennuksen jälkeen. Ohjelma havaitsi, että osassa toimialueen laitteita oli käytössä heikko todennus-protokolla LDAP simple bind (Lightweight Directory Access Protocol), jonka johdosta oli mahdollista, että osan käyttäjien kirjautumistiedot olivat paljastuneet. Kuvassa 18 on esitetty ATA:n ilmoituksen yksityiskohdat-välilehti josta esillä tarkemmat tiedot tapahtuneesta. Heikko protokolla poistettiin myöhemmin käytöstä laitteilta ja sen tilalle otettiin käyttöön Kerberos-todennus.



KUVA 18. Heikon protokollan käytön aiheuttaman varoituksen yksityiskohdat

Tämän lisäksi ATA havaitsi seuranta-aikana muutamia luottosuhteiden katkeamisia, eli laitteiden toimialueesta putoamisia. ATA:n aikajanalla antama ilmoitus tällaisesta on esitetty kuvassa 19, yksityiskohdat piilotettuna. Kuvan alareunassa on myös nähtävissä ATA:n suosittelemat toimenpiteet tilanteeseen, eli tässä tapauksessa laitteen toimialueeseen uudelleen liittäminen tai sen kokonaan poistaminen.



KUVA 19. ATA:n ilmoitus luottosuhteen katkeamisen havaitsemisesta

ATA havaitsi alusta alkaen verkossa myös lähes kaikilta sen laitteilta peräisin olevaa SAMR-protokollan käyttöön liittyvää tiedustelua. Nämä hälytykset kuitenkin todettiin vääriksi, koska hälytyksiä tuli myös uusista vasta-asennetuista laitteista. Microsoft on julkaissut ko. tilanteeseen liittyen ohjeen ATA:n version 1.7 Update 1 päivityksen mukana, jota noudattamalla kaikki väärät hälytykset siirrettiin hylättyjen ilmoitusten osastoon. (Microsoft 2016c.) Hälytysten runsaan määrän vuoksi koko SAMR-seuranta päätettiin kytkeä pois päältä ATA:sta. Tämä onnistui menemällä komentokehotteella sijaintiin: C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin Ja käynnistämällä sieltä tietokanta komennolla:

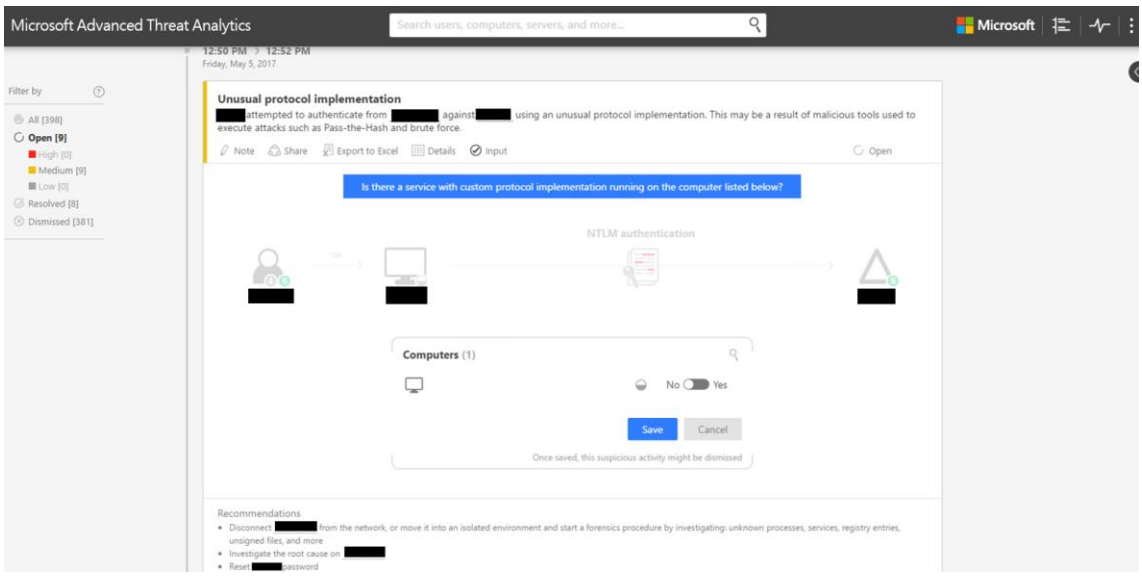
```
”MongoDB.exe ATA”
```

Ja seuraavaksi syöttämällä sille komento:

```
db.SystemProfile.update({_t:"CenterSystemProfile"},
{$set:
{"Configuration.SamrReconnaissanceDetectorConfiguratio
n.IsEnabled":false}})
```

SAMR-seuranta on kuitenkin myöhemmin mahdollista kytkeä takaisin päälle, vaihtamalla komentoon ”Falsen” tilalle ”True”, jos ohjelman tulevat päivitykset vähentävät väärien hälytysten määrää tai hälytysten aiheuttaja WPK-verkossa selvitetään.

Seuranta-ajan lopussa ATA havaitsi myös hyökkäystekniikoiden käyttöä verkossa. Kuvassa 20 esitellään ATA:n hälytys epätavallisesta todennusprotokollan käytöstä, joka saattaa viitata Pass-the-Hash tai Brute Force -hyökkäyksen yritykseen verkossa.



KUVA 20. ATA:n havaitsema NTLM-todennusprotokollan väärinkäyttö

Samaan aikaan ATA ilmoitti myös havainneensa DNS-tiedustelua muutamilta verkon laitteilta. Ohjelman tarjoaman informaation ansiosta hyökkäyksen ja tiedustelun lähteet saatiin nopeasti paikallistettua tietyille verkon laitteille. Kyseessä olevat laitteet olivat tapahtumahetkellä Tampereen ammattikorkeakoulussa järjestetyn tietoturvakoulutuksen kurssilaisten käytössä. Kun asiaa lähdettiin tarkemmin selvittämään, selvisi että kurssilla oli annettu tehtäväksi kokeilla mitä tietoja WPK-verkosta saadaan kaivettua esiin. Verkon ylläpitäjät olivat tietämättömiä harjoituksesta ja tietoturvakurssilaiset olivat tietämättömiä, että ATA oli asennettu verkkoa valvomaan. Tämä ilmoittamaton tiedusteluhyökkäys, vaikkakin oli vain harjoitus, toimi hyvänä odottamattomana testinä ja todisti samalla, että ATA-ohjelmiston konfiguraatio oli verkossa oikein toteutettu.

Seuranta-ajan lopuksi testasin myös itse erilaisten tiedustelutekniikoiden ja houkutus-tunnuksen käyttöä verkossa, jotka ATA myös havaitsi. Testauksessa kävi myös ilmi, että ainakin osalla verkon Windows 7 laitteita on Wdigest-todennus käytössä ja että käyttäjien salasanat ovat näin ollen saatavilla laitteiden muistista selkotekstisinä.

6 POHDINTA

Verizonen raportin mukaan vuonna 2016 tapahtuneista tietorikkomuksista 61% tehtiin yrityksiin, joissa on alle tuhat työntekijää ja 25% rikkomuksista oli sisäpiiriläisten aikaan saamia. 80% hakkerointiin liittyvistä tietorikkomuksista käytti hyväkseen varastettuja tai heikkoja salasanoja. (Verizon 2017.) Tämä osoittaa, että pienemmätkään yritykset eivät ole enää turvassa kyberuhilta ja myös sen, että ihmiset käyttävät edelleen liian heikkoja salasanoja. Se osoittaa myös selvän tarpeen paremmalle käyttäjien valvonnalle, sillä yhä useimmin hyökkääjä löytyy yrityksen sisältä.

Käyttäjien ja kohteiden käyttäytymisanalyysiin perustuvat valvontaohjelmistot ovat suhteellisen tuore teknologia. Tutkimusyhtiö Gartner määritteli sen omaksi markkinakseen vasta vuonna 2015, samoihin aikoihin kuin Microsoft julkaisi Advanced Threat Analytics -ohjelmistonsa. Nämä ns. UEBA-ohjelmistot ovat tehokas tapa valvoa milloin, millä ja miten käyttäjät verkossa toimivat. Käyttäjien valvominen asettaa kuitenkin myös kysymyksen, kuinka paljon käyttäjien toimintaa voidaan valvoa? Tämän määritteleminen on hankalaa, koska yrityksillä täytyy olla oikeus turvata omaisuutensa, mutta samaan aikaan henkilöillä täytyy olla oikeus yksityisyyteensä.

Opinnäytetyön tekeminen oli mittava projekti. Hankaluuksia aiheutti erityisesti työn laajuuden rajaaminen, tietoturvan ollessa laaja ja monisyinen kokonaisuus. Suomenkielistä materiaalia ja ohjeita erilaisten hyökkäystekniikoiden käyttöön ei ollut saatavilla. Tämän vuoksi tässä opinnäytetyössä esitellyt hyökkäysmenetelmien esimerkkitapaukset ja ohjeet pakottivat kirjottajan pohtimaan myös oman työnsä eettisyyttä. Opinnäytetyössä ei kuitenkaan ole salassa pidettävää materiaalia, jolloin se tulee vapaasti kaikkien saataville. Lisäksi kaikki työssä esitelty materiaali on kenen tahansa vapaasti saatavilla englanninkielisenä ja seikkaperäisemmin esitettynä, joten kirjoittaja ei näe ohjeiden esittämistä suomeksi suurena ongelmana.

Toimeksiantajana toiminut tietojenkäsittelyn koulutuksen tutkimus- ja laboratorioverkko WPK tarjosi erinomaisen ympäristön opinnäytetyön konkreettisen osuuden toteutukselle. Microsoftin Advanced Threat Analytics -ohjelmisto saatiin asennettua verkkoa valvomaan ja seuranta-aikana sen tekemien havaintojen pohjalta verkosta saatiin poistettua käytöstä heikko todennusprotokolla. Lisäksi ATA-ohjelmiston avulla

onnistuttiin havaitsemaan tietoturvakurssilaisten toteuttama ilmoittamaton tiedusteluhyökkäysharjoitus lähes heti sen alettua. Seuranta-aikana ATA:sta ei saatu hälytyksiä käyttäjien epänormaalin käytöksen johdosta. Osin tämä saattoi johtua asennusympäristöstä jossa ei ns. toimistoaikoja ollut käytössä, vaan tilat ja laiteet olivat opiskelijoiden käytössä lähes läpi päivän. Lisäksi käyttäjät liikkuvat ympäristössä usein laitteelta toiselle, eikä omia vakiintuneita laitteita ole. Koska ilmoituksia käyttäjien epänormaalista käytöksestä ei saatu, jäi ohjelman havainnointikyky sen osalta selvittämättä.

ATA tarjoaa kokonaisuudessaan valvonnan vain hyvin rajattua toimintaa vastaan. Tarkoittaen, että sen havaitsemat hyökkäystekniikat on hyvin tarkasti määritetty. Sen havainnointikykyä on kuitenkin mahdollista parantaa myöhemmillä päivityksillä. ATA:n asennus on yksinkertainen toteuttaa ja helppokäyttöisen käyttöliittymän ansioista sen käyttäminen ja hallinta eivät vaadi käyttäjältä suurta määrää opiskelua. Tämän ansioista ohjelmisto voidaan asentaa myös pienempiin yrityksiin joissa ei ole suuria IT resursseja.

WPK-verkossa ei ole tällä hetkellä käytössä erillisiä SIEM- ja Syslog-palvelimia, jonka johdosta niiden tarjoamaa tietoliikennettä ei voitu ohjata ATA:lle. Tämän vuoksi ATA:n toteutus jäi hieman vajaaksi ja jotta ohjelmistosta saataisiin paras hyöty irti ja verkko mahdollisimman hyvin valvottua, tulisi tällaiset palvelut toteuttaa verkossa. Tämän lisäksi ohjelmiston konfiguraatiota voi edelleen kehittää lisäämällä houkutus-tunnuksia ja ottamalla hälytysten sähköposti-ilmoitukset käyttöön.

Windows 10 -käyttöjärjestelmä sisältää uuden ”Credential Guard” -ominaisuuden, joka luo käyttäjätunnuksille ja salasanan tiivisteille oman virtuaalisen säilytystilan. Tämä ominaisuus estää opinnäytetyössä esiteltyjen kirjautumistietojen varastamistekniikoiden toteuttamisen Mimikatzin kaltaisten työkalujen avulla, koska tietoja ei enää tallenneta laitteen RAM-muistiin. Kyseinen ominaisuus on saatavilla ainoastaan Windowsin 10 Enterprise versiossa ja se on erikseen konfiguroitava. WPK-verkossa oli tämän työn kirjoitushetkellä koekäytössä vain muutamia Windows 10 Enterprise -käyttöjärjestelmällä varustettuja laitteita, pääosan laitteista käyttäessä vielä vanhempia 7 ja 8.1 versioita. Windows 10 -käyttöjärjestelmä on huomattavasti paremmin suojattu tässä opinnäytetyössä esitettyjä erilaisia käyttäjätunnusvarkaustekniikoita vastaan ja kirjoittaja suosittelee WPK-verkon kaikkien laitteiden päivittämistä Windows 10 -käyttöjärjestelmään nopealla aikataululla.

Välittömänä toimena kirjoittaja suosittelee Wdigest-todennuksen käytöstä poistamista verkossa, jotta käyttäjien selkotekstisiä salasanoja ei voida varastaa Windows 7 -laitteiden muistista. Tämän lisäksi verkossa tulisi selvittää NTLM-todennuksen käytöstä poistamisen mahdollisuutta ja selvittää voitaisiinko kaikki todennus toteuttaa ainoastaan uudempaa Kerberos-protokollaa käyttäen.

Mikään tietoturvaratkaisu ei voi taata täydellistä suojaa kyberuhilta, mutta monessa yrityksessä ja organisaatiossa asiat tehdään hyökkääjälle liian helpoksi, jättämällä päivitykset ja muut tarvittavat toimet tekemättä. Myös verkon käyttäjien valistuksella on edelleen merkittävä vaikutus siihen, kuinka helposti verkkoon voidaan tunkeutua. Hyvä tietoturva on monen tekijän yhteisvaikutuksen tulos ja se vaatii kaikkien panosta.

LÄHTEET

Abernathy, R. & McMillian, T. 2016. CISSP Cert Guide, Second Edition. 2. painos. USA: Pearson Education, Inc. Vaatii käyttöoikeuden. http://proquest.safaribooksonline.com.elib.tamk.fi/book/certification/cissp/9780134174129

Barret, D., Weiss, M. & Hausman, K. 2015. CompTIA Security+ SYO-401 Exam Cram. Fourth Edition. 5. painos. USA: Pearson Education, Inc. Vaatii käyttöoikeuden. http://proquest.safaribooksonline.com.elib.tamk.fi/book/certification/securityplus/9780133836455

Cloppert, M. 14.11.2009. Security Intelligence: Attacking the Cyber Kill Chain. Luettu: 9.4.2017. https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain

Delby, B. 7.9.2014. Mimikatz Github. Luettu: 6.5.2017. https://github.com/gentilkiwi/mimikatz/wiki

Diogenes, Y., Gilbert J. & Mazzoli, R. 2016. Enterprise Mobility with App Management, Office 365, and Threat Mitigation: Beyond BYOD. 1. painos. Washington: Microsoft Press.

Donaldson, S., Siegel, S., Williams, C. & Aslam, A. 2015. Enterprise Cybersecurity: How to Build Successful Cyberdefence Program Against Advanced Threats. 1. painos. New York: Apress Media, LLC.

Easttom, C. 2016. Computer Security Fundamentals, Third Edition. 1. painos. Indianapolis: Pearson Education, Inc.

EC-Council. 2010. Ethical Hacking and Countermeasures: Attack Phases. 1. painos. USA: EC-Council Press.

Engel, G. 18.11.2014. Deconstructing the Cyber Kill Chain. Luettu 14.2.2017. http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542

Falde, K. 1.11.2014. KB2871997 and Wdigest – Part 1. Luettu: 3.5.2017. https://blogs.technet.microsoft.com/kfalde/2014/11/01/kb2871997-and-wdigest-part-1

Gregg, M. 2016. CISSP Exam Cram, Fourth Edition. 1. painos. USA: Pearson Education, Inc. Vaatii käyttöoikeuden. http://proquest.safaribooksonline.com.elib.tamk.fi/book/certification/cissp/9780134209555

Greiner, L. 19.1.2015. The Skeleton (key) in your closet: Malware Allowing Attackers to Infiltrate Corporate Networks. Luettu: 11.4.2017. http://business.financialpost.com/fp-tech-desk/cio/the-skeleton-key-in-your-closet-malware-allowing-attackers-to-infiltrate-corporate-networks

Gordon, A. 2015. Official CISSP (ISC)² CBK, Fourth Edition. 1. painos. Boca Raton: CRC Press. Vaatii käyttöoikeuden. http://proquest.safaribooksonline.com.elib.tamk.fi/book/certification/cissp/9781482262759

Greene, T. 5.8.2016. Why the 'cyber kill chain' needs an upgrade. Luettu: 15.3.2017. http://www.networkworld.com/article/3104542/security/why-the-cyber-kill-chain-needs-an-upgradesecurity-pros-need-to-focus-more-on-catching-attackers-aft.html

Grimes, R. 19.8.2014. Fear the Golden Ticket Attack. Luettu: 6.5.2017. http://www.infoworld.com/article/2608877/security/fear-the-golden-ticket-attack-.html

Harris, A., Zilberstein, G. & Zinger, A. 16.2.2017. Advanced Threat Analytics Attack Simulation Playbook v.1.0. Luettu: 28.3.2017. https://gallery.technet.microsoft.com/Advanced-Threat-Analytics-8b0a86bc

Hutchins, E., Cloppert, M., Amin, R. 2011. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Luettu 11.2.2017. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Johansson, J. 2006. Security Watch: The Most Misunderstood Windows Security Settings of All Time. Luettu: 18.2.2017. https://technet.microsoft.com/en-us/library/2006.08.securitywatch.aspx

Jungles, P., Simos, M., Grimes, R., Margosis, A. & Robinson, L. 2012. Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft. Luettu: 18.2.2017. https://www.microsoft.com/en-us/download/details.aspx?id=36036

Karkimo, A. 22.3.2017. F-Securen testin masentava tulos: joka toinen lankesi huijausviestiin. Luettu: 4.4.2017. http://www.tivi.fi/Kaikki_uutiset/f-securen-testin-masentava-tulos-joka-toinen-lankesi-huijausviestiin-6634948

Lincoln, B. 19.12.2014. Mimikatz 2.0 – Golden Ticket Walkthrough. Luettu: 6.5.2017 http://www.beneaththewaves.net/Projects/Mimikatz_20_-_Golden_Ticket_Walkthrough.html

Mandiant Intelligence Center. 18.2.2013. APT1 Exposing one of China's cyber espionage units. Luettu. 18.2.2017. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

McNab, C. 2016. Network Security Assessment, 3rd Edition. 1. painos. Sebastopol: O'Reilly Media, Inc. Luettu: 5.5.2017. Vaatii käyttöoikeuden. http://proquest.safaribooksonline.com.elib.tamk.fi/book/networking/security/9781491911044

Metacalf, S. 5.5.2016. Unofficial Guide to Mimikatz & Command Reference. Luettu: 6.5.2017. https://adsecurity.org/?page_id=1821

Microsoft. n.d. Microsoft NTLM. Luettu: 25.2.2017. https://msdn.microsoft.com/en-us/library/windows/desktop/aa378749(v=vs.85).aspx

Microsoft. 2016a. Advanced Threat Analytics Documentation. Luettu: 11.2.2017. https://docs.microsoft.com/en-us/advanced-threat-analytics

Microsoft. 2016b. [MS-NLMP]: NT LAN Manager (NTLM) Authentication Protocol. Luettu: 25.2.2017. https://msdn.microsoft.com/en-us/library/cc236621.aspx

Microsoft. 2016c. Description of Update 1 for Microsoft Advanced Threat Analytics 1.7. Luettu: 4.5.2017. https://support.microsoft.com/en-us/help/3191777/description-of-update-1-for-microsoft-advanced-threat-analytics-v1.7

Microsoft. 2015. Microsoft Advanced Threat Analytics Licensing Datasheet. Luettu: 31.5.2017. https://www.microsoft.com/fi-fi/cloud-platform/advanced-threat-analytics-pricing

Numoto, T. 13.11.2014. Microsoft Acquires Aorato to Give Enterprise Customers Better Defense Against Digital Intruders in a Hybrid Cloud World. Luettu: 4.5.2017. https://blogs.microsoft.com/blog/2014/11/13/microsoft-acquires-aorato-give-enterprise-customers-better-defense-digital-intruders-hybrid-cloud-world/

O´Leary, M. 2015. Cyber Operations: Building, Defending, and Attacking Modern Computer Networks. 1. painos. New York: Apress Media, LLC.

Perlroth, N. 22.4.2013 The Year in Hacking, by the Numbers. Luettu: 26.5.2017. https://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/?_r=0

Pilkington, M. 24.11.2014. Kerberos in the Crosshairs: Golden Tickets, Silver Tickets, MITM, and More. Luettu: 4.5.2017.https://digital-forensics.sans.org/blog/2014/11/24/kerberos-in-the-crosshairs-golden-tickets-silver-tickets-mitm-more

Regan, P. 2014. Administering Windows Server 2012 R2. 1. painos. USA: John Wiley & Sons, Inc.

Saydag, B. & Moore, S. 2015. Defeating Pass-the-Hash Separation of Powers. Luettu: 11.2.1017. https://www.blackhat.com/docs/us-15/materials/us-15-Moore-Defeating%20Pass-the-Hash-Separation-Of-Powers-wp.pdf

Schneier, B. 2015. Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition. 1. painos. USA: John Wiley & Sons, Inc. Vaatii käyttöoikeuden. http://proquest.safaribooksonline.com.elib.tamk.fi/book/software-engineering-and-development/cryptography/9781119096726

Simons, A. 4.5.2015. Microsoft Advanced Threat Analytics Public Preview Release is Now Available! Luettu: 4.5.2017. https://blogs.technet.microsoft.com/enterprisemobility/2015/05/04/microsoft-advanced-threat-analytics-public-preview-release-is-now-available

TechNet. 2015. Command-line Reference. Luettu: 16.2.2017. https://technet.microsoft.com/en-us/library/cc754340(v=ws.11).aspx

TechNet. 2014. Windows Authentication Overview. Luettu: 11.2.2017. https://technet.microsoft.com/en-us/library/hh831472

TechNet. 2013. Windows Authentication Concepts. Luettu: 11.2.2017. https://technet.microsoft.com/library/dn169018.aspx

TechNet. 2012. NTLM Overview. Luettu: 11.2.2017 https://technet.microsoft.com/en-us/library/hh831571.aspx

Tomonaga, S. 26.1.2016. Windows Commands Abused by Attackers. Luettu: 11.2.2017. http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html

Trull, J. 28.11.2016. Disrupting the Kill Chain. Luettu: 11.2.2017. https://blogs.microsoft.com/microsoftsecure/2016/11/28/disrupting-the-kill-chain

Velazquez, C. 30.8.2015. Detecting and Preventing Attacks Earlier in the Kill Chain. Luettu: 18.2.2017. https://www.sans.org/reading-room/whitepapers/infosec/detecting-preventing-attacks-earlier-kill-chain-36230

Verizon. 2017. 2017 Data Breach Investigation Report. Luettu: 28.5.2017 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017

Wu, C-H. & Irwin, J. 2013. Introduction to Computer Networks and Cybersecurity. 1. painos. Boca Raton: CRC Press.