Aktiivihakemiston salasanojen auditointi

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Visamäki, tietojenkäsittelyn koulutusohjelma

Syksy, 2018

Joona Kuittinen

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutusohjelma
Visamäki

Tekijä Joona Kuittinen **Vuosi** 2018

Työn nimi Aktiivihakemiston salasanojen auditointi

Työn ohjaaja Erkki Laine

TIIVISTELMÄ

Opinnäytetyössä perehdyttiin salasana-auditointiin Windows-aktiivihakemistoympäristössä. Tavoitteena oli tutustua menetelmiin, joilla salasana-auditointi toteutetaan. Työssä sovellettiin vuonna 2017 julkaistuja uusia salasanakäytäntöjä, ja testiympäristönä käytettiin Windows Server 2016 -palvelinkäyttöjärjestelmää, johon oli asennettu aktiivihakemistopalvelu. Testiympäristössä oli yli kaksisataa käyttäjätunnusta, joille oli luotu sekä turvallisia että heikkoja salasanoja.

Opinnäytetyön lähteinä hyödynnettiin kirjallisia lähteitä ja virallisia dokumentaatioita. Lähdemateriaalista koostettiin kokonaisuus, jonka avulla saadaan yleiskuva tietoturva-auditoinnista, salasanoista ja niiden murtamisesta, aktiivihakemistosta ja salasanojen roolista aktiivihakemistossa.

Käytännön osuudessa salasanat sisältävät tiedostot kopioitiin aktiivihakemistosta ja siirrettiin tietokoneelle, jolla salasanojen murtaminen toteutettiin. Salasanojen murtaminen suoritettiin käyttämällä yleisimpiä murtamismenetelmiä.

Johtopäätöksissä todettiin, että salasanojen auditointi tiettyä menetelmää käyttämällä on tehokkaampaa kuin toisilla menetelmillä, ja tietyt menetelmät soveltuvat paremmin tiettyihin tarkoituksiin. Tuloksissa pohdittiin myös sitä, onko uusien salasanakäytäntöjen käyttäminen sellaisenaan riittävää.

Avainsanat Salasana-auditointi, salasanat, tietoturva, Windows Server 2016, aktiivihakemisto

Sivut 29 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Visamäki

Author Joona Kuittinen **Year** 2018

Subject Active Directory Password Auditing

Supervisor Erkki Laine

ABSTRACT

The objective of this thesis was to become familiar with password auditing in Windows Active Directory environment, by studying methods that are used in password auditing. The new password guidelines released in 2017 were applied in this thesis. The auditing environment consisted of Windows Server 2016 server operating system with Active Directory service installed, and over two hundred user accounts with weak and strong passwords.

Sources of information in this thesis were written works and official documentations. The source material was compiled together to form an overview of IT security auditing, passwords and methods used to crack them, active directory and role of passwords in the active directory.

In the practical part of this thesis, the files in active directory containing the passwords were extracted and moved to a computer, which was used to crack the passwords. The passwords were cracked by using the most common cracking methods.

The conclusions illustrate that password auditing using a particular method was more efficient than by other methods, and that certain methods are more suitable for specific purposes. The results also considered whether the use of the new password guidelines used as such is sufficient enough.

Keywords Password auditing, passwords, information security, Windows Server 2016, Active Directory

Pages 29 pages

SISÄLLYS

1 JOHDANTO

Yhdysvaltojen kansallinen standardien ja teknologian instituutti (NIST) julkaisi kesällä 2017 uudet salasanakäytännöt, jotka laittoivat salasanojen vaatimukset uusiksi. Salasanoille annetaan vain yksi vaatimus: sen tulee olla pitkä. Nämä käytännöt antavat käyttäjälle enemmän vapauksia salasanan luomisessa. Koska käyttäjille annetaan paljon vapautta salasanan valintaan, salasanoja täytyy jollain tapaa valvoa, ettei huonoksi todettuja salasanoja käytetä. Huonoksi todettuja salasanoja ovat helposti arvattavat sekä aikaisemmissa tietomurroissa vuotaneet salasanat.

Salasanat ovat monissa organisaatioissa yleisin tapa todentaa käyttäjä ja monet organisaatiot käyttävät aktiivihakemistoa, joka varastoi salasanoja heikkojen salausalgoritmien takana. Tässä opinnäytetyössä tutkitaan tapoja toteuttaa salasanojen vahvuuden arviointi, eli auditointi. Työ toteutetaan Windows Server 2016 -aktiivihakemistossa järjestelmänvalvojan näkökulmasta. Työtä varten luotiin pienen organisaation aktiivihakemistoa simuloiva ympäristö, jossa on useita käyttäjiä. Työssä käytetään ilmaiseksi saatavilla olevia ohjelmistotyökaluja.

Idea opinnäytetyöhön tuli tutustuessa NISTin uuteen salasanasuositukseen, jossa salasanojen vahvuuden arvioimiseen suositeltiin salasana-auditointia. Yhdistämällä salasana-auditoinnin ja Windows-aktiivihakemiston sain opinnäytteen aiheeksi työn, jossa pääsen tutustumaan tietoturvaan sekä Windows-palvelinympäristöön.

Opinnäytetyön tutkimuskysymykset olivat: Mitä tuloksia salasana-auditoinnilla halutaan saavuttaa? Mikä on tehokkain tapa toteuttaa salasana-auditointi? Työn teoreettisessa osiossa vastataan ensimmäiseen tutkimuskysymykseen ja esitellään aktiivihakemiston salasanojen auditointiin liittyviä järjestelmiä ja prosesseja. Käytännön osuudessa pyritään salasanojen murtamismenetelmiä soveltamalla vastaamaan toiseen tutkimuskysymykseen. Lopputuloksena esitellään parhaaksi todettu tapa toteuttaa salasana-auditointi.

2 TIETOTURVA-AUDITOINTI

Pelkkä tietoturvakäytäntöjen ja -prosessien käyttäminen ei takaa sitä, että organisaation arkaluontoiset ja salaiset tiedot, kuten henkilötiedot ja erilaiset sopimukset, ovat turvassa. Tietoturvakäytännöt eivät välttämättä ole riittäviä tai niitä ei noudateta asianmukaisesti. Käytäntöjen tehokkuuden varmistamiseksi niiden tavoitteet sekä vaikutus tulee arvioida esimerkiksi auditoimalla. (IntiGrow 2018.)

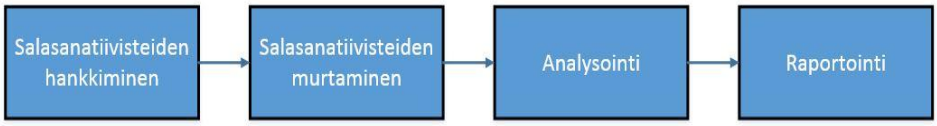
Auditointi on henkilön, organisaation, järjestelmän, prosessin, projektin tai tuotteen arviointia, joka toteutetaan informaation paikkansapitävyyden ja luotettavuuden todentamiseksi. Tietoturva-auditoinniksi kutsutaan kaikkea auditointia, joka sisältää tietojärjestelmien ja niihin liittyvien prosessien ja rajapintojen tarkastuksen sekä arvioinnin. Tietoturva-auditointi sisältää erilaisten menetelmien käyttämistä tiedon keräämiseen ja kerätyn tiedon vertailemiseen ennalta määriteltyjen standardien mukaisesti. Tarkoituksena on varmistaa, että käytetyt menetelmät ja infrastruktuurit ovat sopivia sekä ajan tasalla. Tietoturva-auditointi auttaa myös varmistamaan, että organisaatio ei vahingossa aiheuta tietotekniikkaan liittyviä riskejä tai uhkia muille organisaatioille epäpätevien käytäntöjen ja huonon hallinnan takia. Näitä uhkia ovat tietoturvamurrot, teollisuusvakoilu tai -sabotaasi, roskapostitus, häirintä ja yksityisyyden loukkaukset. (Bosworth, Kabay, Whyne 2014, 1527.)

Tietoturva-auditoinnin voi toteuttaa joko ulkoisesti tai sisäisesti. Ulkoinen auditointi on formaali prosessi, jonka suorittaa sertifioitu auditointiammattilainen keskittyen varmistamaan, että organisaation sisäisiä käytäntöjä, ulkoisia standardeja ja laillisia vaatimuksia noudatetaan. Sisäistä auditointia kutsutaan arvioinniksi (assessment). Arviointi on epävirallinen prosessi ja sen suorittaa alan ammattilainen, jonka ei tarvitse olla sertifioitu auditoija. Arvioinnissa keskitytään parantamaan tehokkuutta ja toimivuutta käyttäen useimmiten epävirallisia alan suosituksia ja arvioijan ammattiosaamista. (Boshworth 2014, 1527.)

Yksi hyvä tapa demonstroida tarvetta paremmille salasanoille on näyttää ihmisille, kuinka helposti heidän salasanansa ovat murrettavissa. MacGregor (2002) kertoo, että monilla ihmisillä ei ole käsitystä siitä, miten helposti saatavilla ja helppokäyttöisiä salasanan murtamiseen käytetyt työkalut ovat. Yhden helposti arvattavan salasanan kompromissi saattaa kiertää tietoturva-asetukset, ajan tasalla olevat päivitykset ja tiukat palomuuriasetukset tehokkaammin kuin minkään haavoittuvuuden käyttäminen. Kaikki salasanat voidaan murtaa ennemmin tai myöhemmin. Tarkoituksena on tehdä salasanasta tarpeeksi monimutkainen, että hyökkääjä antaa periksi ennen kuin salasana on saatu murrettua.

Auditoimalla organisaation käyttäjätunnuksien salasanoja saadaan arvioitua, noudattavatko käyttäjät organisaation salasanakäytäntöjä sekä testattua salasanojen vahvuuksia. Tämä auttaa luomaan ympäristön, joka on vähemmän altis murroille heikkojen salasanojen takia. Tuloksena heikot salasanat saadaan poistettua käytöstä ja käyttäjiä opastettua luomaan turvallisempia salasanoja. Useimmiten järjestelmänvalvojat käyttävät salasanojen vahvuuden testaamiseen samoja työkaluja kuin hyökkääjät. (Gibson 2015, 465.)

Windows-aktiivihakemiston salasana-auditoinnin ensimmäinen vaihe on salasanoista muodostettujen salasanatiivisteiden hankkiminen. Tähän voidaan käyttää Microsoftin tai kolmansien osapuolten työkaluja. Salasanatiivisteiden hankkimisen jälkeen salasanatiivisteitä yritetään murtaa käyttäen yhtä tai useampaa menetelmää. Tulokset salasanatiivisteiden murtamisesta analysoidaan ja johtopäätökset raportoidaan. Analysoinnissa voidaan katsoa esimerkiksi murrettujen salasanatiivisteiden vahvuuksia tai kuinka monta prosenttia organisaation salasanoista saatiin murrettua. Kuvassa 1 on esitettynä salasana-auditointiprosessi. (Boller 2017, 2-3.)



Kuva 1. Salasana-auditointiprosessi.

3 SALASANAT

Salasana on pelkistä kirjaimista, numeroista, erikoismerkeistä tai näiden yhdistelmistä koostuva merkkijono, jota käytetään vahvistamaan käyttäjän identiteetti. Digitalisuuden aikakautena salasanat toimivat tärkeässä roolissa. Ne suojaavat käyttäjiä ulkopuolisten luvattomalta pääsyltä heidän sähköpostiinsa, käyttäjätunnukselle, verkkosivustoonsa, verkkopankkiinsa tai laitteistoonsa, esimerkiksi verkkomodeemeihin.

Turvallisen salasanan luontia monimutkaistaa tasapainottelu salasanan murrettavuuden vaikeuden sekä helppokäyttöisyyden välillä. Todellisesti satunnaiset salasanat ovat vaikeita muistaa, ja käyttäjien itse valitsemat salasanat ovat ennalta arvattavia. Organisaatiot voivat yrittää tasapainotella näiden kahden tavoitteen välillä esimerkiksi pakottamalla käyttäjän käyttämään erikoismerkkejä salasanassaan tai tietyn pituista salasanaa käyttämällä salasanakäytäntöjä. Tämä ei kuitenkaan auta luomaan vaikeammin arvattavia salasanoja. (Weir, Aggarwal, Collins & Stern 2010.)

Floridan yliopiston tutkimuksessa (Weir ym. 2010) saatiin selville, että käyttäjät useimmiten kapitalisoivat salasanan ensimmäisen kirjaimen ja lisäävät joko numeron ”1” tai huutomerkin, ”!”, salasanan loppuun tehdäkseen siitä vaikeammin murrettavan. Aikaisemmista tietovuodoista saaduista salasanalistoista nähtiin, että kun salasanassa vaadittiin numeroiden käyttöä, 70 % käyttäjistä lisäsivät numeron ennen salasanaa tai sen jälkeen. Salasanojen murtamiseen käytetyt ohjelmistot pystyvät helposti ennustamaan tällaisen käytöksen.

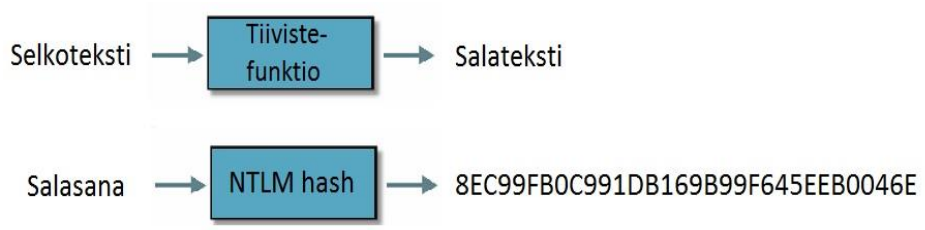
Viestintäviraston (n.d.) mukaan salasanan vähimmäispituuden tulisi olla 15 merkkiä. Pituus suojaa salasanaa teknisiltä sekä sosiaalisilta huijauksilta, sillä pitkä salasana on vaikea arvata ja sen tiivisteen selvittäminen vie paljon resursseja, kuten aikaa. Salasanojen eli yksittäisten sanojen käyttäminen salasanana tulisi viestintäviraston mukaan unohtaa, ja ihmisten pitäisi alkaa käyttämään salalauseita. Salalauseessa kahta tai useampaa sanaa yhdistelemällä saadaan luotua vaikeammin arvattavissa ja murrettavissa oleva salasana.

Salasanojen hallinnan helpottamiseksi voidaan käyttää salasanojen hallintasovelluksia. Hallintasovelluksessa kaikkia käyttäjän salasanojen säilötään yhden pääsalasanan takana. Tämän ansiosta käyttäjän tarvitsee muistaa vain yksi salasana. Salasanojen hallintasovelluksilla voidaan myös luoda vahvoja ja laskelmallisesti hyvin vaikeasti murrettavissa olevia salasanoja. (Viestintävirasto n.d.)

3.1 Tiivistealgoritmit

Termiä selkoteksti (engl. plaintext) käytetään kryptografiassa kuvailemaan salaamatonta tekstiä tai tietoa. Kun selkoteksti salataan käyttämällä jotakin salausalgoritmia, siitä tulee salatekstiä (engl. ciphertext). Tietokonejärjestelmät eivät normaalisti säilytä käyttäjien salasanoja, vaan tiivisteitä näistä salasanoista. Salasanan tiivistäminen on yksi peruskäsitteistä suunnitellessa mitä tahansa käyttäjien salasanoja vastaanottavaa palvelua. Ilman salasanan tiivistämistä kaikki palvelun tietokantaan tallennetut salasanat ovat selkotekstimuodossa. Kun tiivistealgoritmia käytetään käyttäjien salasanoihin ennen niiden tallentamista tietokantaan, salasanat tallentuvat tietokantaan salatekstinä. Hyökkääjä ei pysty suoraan käyttämään salasanoja, vaan salateksti tulee murtaa. (Gibson 2015, 611.)

Tiiviste (engl. hash) on yksisuuntainen matemaattinen funktio (kuva 2). Funktion tarkoitus on tehdä matemaattinen toimenpide, joka on helppo suorittaa, mutta lähes mahdoton peruuttaa. Kuten muut salaustekniikat, tiivistäminen muuttaa selkotekstin salatekstiksi. Vaikka tietyissä salaustekniikoissa tiedon voi muuttaa salatekstistä takaisin selkotekstiksi tietyllä avaimella, tiivisteitä ei ole suunniteltu purettavaksi. Esimerkiksi käyttäjän kirjautuessa salasanalla palveluun järjestelmä luo syötetystä salasanasta tiivisteen ja vertaa sitä tietokannassa olevaan tiivisteeseen, vahvistaen salasanan paikkansapitävyyden. (Greenberg 2016.)



Kuva 2. Tiivistysprosessi NTLM-tiivistefunktiolla.

Koska tietty salasana tuottaa aina tietyn tiivisteen, salasanan selvittäminen tiivisteestä on mahdollista esimerkiksi vertailemalla tiivistettä listaan valmiita tiivisteitä ja niitä vastaaviin selkoteksteihin. Tiivisteestä voidaan luoda vahvempi käyttämällä suolaa (engl. salt), joka on joukko satunnaisia bittejä. Suola lisätään salasanaan ennen salasanan tiivistämistä. (Gibson 2015, 611.)

3.2 **NIST 800-63B -suositus**

National Institute of Standards and Technology (NIST) on Amerikan Yhdysvaltojen kauppaministeriön kansallinen standardoinnin ja teknologian virasto. Sen tehtävänä on edistää innovaatiota ja teollista kilpailukykyä kehittämällä mittaustekniikoita, teknologioita ja standardeja tavoilla, jotka parantavat yleistä elämisen tasoa sekä taloudellista turvaa. (PasswordPing n.d.)

NIST kehittää valtakunnallisia informaation prosessointistandardeja (Federal Information Processing Standards – FIPS), joille kauppaministeriö antaa hyväksynnän ja joita valtakunnallisten virastojen tulee käyttää. NIST tarjoaa myös ohjeistusdokumentteja sekä suosituksia Special Publications (SP) 800 -sarjan kautta. Teknologiateollisuudessa nämä suositukset otetaan usein parhaiden käytäntöjen peruspilareiksi ja liitetään muihin standardeihin. (PasswordPing n.d.)

Kesällä 2017 NIST julkaisi viimeistellyn 800-63B-suosituksen (NIST 2017), joka uusii salasanakäytännöt täysin. Suosituksen tarkoituksena on saada käyttäjät luomaan turvallisempia salasanoja tähtäämällä käyttäjäystävällisyyteen ja siirtämällä salasanan vahvuuden varmentaminen palveluntarjoajalle aina kun mahdollista. Jotta salasana olisi mahdollisimman käyttäjäystävällinen, 800-63B suositus tarjoaa useamman pääperiaatteen. (Maida 2016.)

800-63B suosituksen mukaan salasanan ehdoton minimipituus on 8 merkkiä ja maksimipituuden tulee olla enemmän kuin 64 merkkiä. Salasanassa tulisi sallia kaikki ASCII- ja Unicode-merkit, kuten välilyönnit ja hymiöt. Salasanoja tulee auditoida eikä yleisiä, helposti arvattavia sanakirjasta löytyviä sanoja kuten *salasana* tai *helsinki*, saisi sallia. Monimutkaisuusvaatimuksista ja salasanan vanhenemiskäytännöistä täytyy päästä eroon, sillä niiden käyttäminen johtaa heikkojen salasanojen luomiseen. Salasanojen uusiminen tulee pakottaa ainoastaan tietomurron tapahtuessa. (Maida 2016.)

3.3 **Salasanojen murtaminen**

Salasanojen murtamisella tarkoitetaan prosessia, jonka avulla salatekstiksi muutettu salasana saadaan muutettua takaisin selkotekstiksi. Salasanojen murtaminen sisältää kaksi vaihetta. Ensimmäisenä on saatava käsiin salasanojen tiivisteet sisältävä tiedosto. Tämän jälkeen tiivisteet yritetään murtaa käyttämällä yhtä tai useampaa salasanan murtamismenetelmää. (Gibson 2015, 256.)

Tässä työssä murtamismenetelminä käytetään brute force-, sanakirja- ja rainbow table -menetelmiä. Nämä ovat yleisimpiä menetelmiä salasanojen murtamiseen.

Brute force-menetelmä on perusteellisin tapa murtaa salasanoja. Siinä kokeillaan jokaista mahdollista kirjaimista, numeroista ja erikoismerkeistä koostuvaa permutaatiota salasanana. Tämä menetelmä on erittäin hidas, kun salasana on pitempi kuin 8 merkkiä, sillä se luottaa täysin tietokoneen laskentatehoon ja toistoon. Tämän takia ei ole soveliasta käyttää brute force -menetelmää yli 8-merkkisiin salasanoihin, ellei käytössä ole salasanojen murtamiseen tarkoitettua näytönohjainfarmia, joka koostuu useasta korkeatasoisesta näytönohjaimesta. Tästä huolimatta brute force -menetelmä on ainoa menetelmä, joka takaa oikean salasanan tuottamisen ajan myötä. (Parikh 2013, 19.)

Brute force -menetelmän soveltuvuus riippuu salausavaimen pituudesta sekä saatavilla olevasta laskentatehosta. Mahdollisten permutaatioiden määrä voidaan laskea kuvassa 3 esitetyllä kaavalla.

$$KS = L^{(m)} + L^{(m+1)} + L^{(m+2)} + \ldots\ldots + L^{(M)}$$

KS	Key Space, avaimen kaikki permutaatiot
L	Merkistön koko
m	Avaimen minimipituus
M	Avaimen maksimipituus

Kuva 3. Permutaatioiden määrän laskentakaava. (Parikh 2013, 19.)

Sanakirja-menetelmässä, englanniksi Dictionary Attack, salasana yritetään murtaa käyttämällä ennalta koottuja sanalistoja. Sanalista voi koostua esimerkiksi yleisimmin käytetyistä salasanoista, yleisistä aluekohtaisista sanoista, asuinpaikoista, tavaramerkeistä, urheilujoukkueista ja tietomurtojen kautta vuodetuista salasanalistoista. (Parikh 2013, 21.)

Sanakirja-menetelmä on hyvin tehokas, sillä ihmisillä on tapana valita salasanaksi kohtuullisen lyhyitä ja normaaleja sanakirjasta löytyviä sanoja, jotka on helppo muistaa. Jos salasana on tarpeeksi monimutkainen, eikä se ole vuotanut aikaisemmissa tietovuodoissa, sitä ei sanakirja-menetelmällä pystytä murtamaan. (Parikh 2013, 21.)

Sanakirja-menetelmään voidaan myös yhdistää brute force -menetelmästä toiston ominaisuus, missä sanojen eteen ja/tai perään lisätään numerosarjoja. Esimerkiksi jos sanan ”salasana” perään lisätään numeroarvoja viiden merkin edestä, saadaan testattua kaikki salasanat, salasana0 ja salasana99999, välillä. Ihmisillä on tapana lisätä sanojen perään vuosilukuja, mikä tekee tästä menetelmästä hyvin tehokkaan. Tällaista menetelmää kutsutaan hybrid-menetelmäksi. (Parikh 2013, 22.)

Rainbow table -menetelmässä käytetään hyväksi niin sanottuja esilaskettuja rainbow tableja. Rainbow table on suuri tietokanta, joka koostuu suuresta määrästä jonkin tiivistefunktion tuottamista tiivisteistä ja näiden tiivisteiden tulosteista. Rainbow table -tietokannan käyttäminen tekee salasanatiivisteen brute forcettamisesta helpompaa poistamalla brute forcesta laskennallisesti hankalimman osuuden, eli itse tiivistefunktion toteuttamisen. Koska kaikki mahdolliset tiivistearvot on laskettu valmiiksi, rainbow table -menetelmässä toteutetaan yksinkertainen etsi ja vertaa -toimenpide salasanalistaa vastaan. (LearnCryptography n.d.)

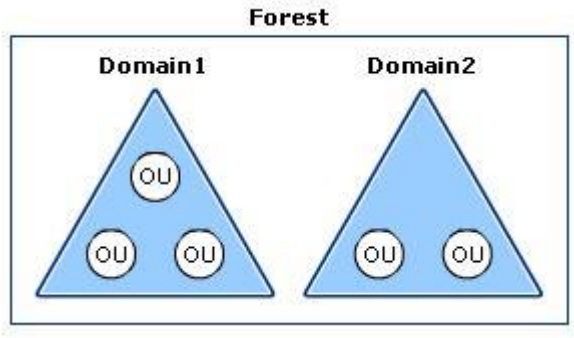
Rainbow tableilla on myös omat heikkoutensa. Jos tiiviste, jota yritetään murtaa, ei ole rainbow tablessa, sitä ei yksinkertaisesti saada murrettua. Rainbow table -menetelmää käyttäessä rajoitteena on käytössä oleva rainbow table. Tiivistetietokantojen luominen vaatii paljon laskennallisia resursseja, sillä kaikki mahdolliset tiivisteet ja niiden tulosteet täytyy laskea. Tämän takia näitä tietokantoja harvoin valmistetaan itse, vaan useimmiten käytetään valmiiksi laskettuja tiivistetietokantoja. Rainbow tableja rajoittaa myös niiden koko – nopeus, joka saavutetaan käyttämällä esilaskettuja tiivisteitä, maksetaan sillä, että joudutaan säilyttämään erittäin suurikokoisia tiedostoja. Esimerkiksi rainbow table, joka pitää sisällään yli kuusi kvadriljoonaa NTLM-tiivistefunktion tuottamaa tiivistettä 1-8 merkkiä pitkistä salasanoista, vie tilaa 460 gigatavun verran. (LearnCryptography n.d.)

Rainbow table -menetelmä oli hetken aikaa hyvin tehokas tapa murtaa salasanoja. Tarpeeksi suurella tiivistetietokannalla oikean salasanan löytämisen todennäköisyys oli hyvin korkea, mikä johtui käytössä olevista tiivistealgoritmeista ja helposti saatavilla olevista usein käytetyistä salasanoista koostuvista tiivistetietokannoista. Nykypäivänä tiivistealgoritmit ovat kehittyneet ja erityisesti suolan lisääminen ennen tai jälkeen tiivistämisen on tullut yleiseksi käytännöksi, mikä vaikeuttaa rainbow tablen luomista. (LearnCryptograhy n.d.) Moderneilla näytönohjaimilla erikoismerkitön 8 merkkiä pitkä salasana voidaan murtaa muutamissa minuuteissa käyttäen puhdasta brute force -menetelmää, mikä tekee useiden satojen gigatavujen kokoisista rainbow tableista epäkäytännöllisiä.

4 WINDOWS AKTIIVIHAKEMISTO

Aktiivihakemisto, englanniksi Active Directory, on hakemistopalvelu, joka tarjoaa hallintamahdollisuuden Windows-järjestelmille, -applikaatioille, ja -verkoille. Aktiivihakemistoa käytetään pääosin säilyttämään tietoa Windows-ympäristön verkko-objekteista, joita ovat käyttäjät, ryhmät, järjestelmät, verkot ja applikaatiot, rakenteellisessa hierarkiassa, joka on suunniteltu hallitsemaan käyttäjien käyttöoikeuksia. Tämä malli sallii järjestelmänvalvojien varmistaa, että oikea käyttäjä pääsee käsiksi oikeaan resurssiin oikeaan aikaan, samalla tarjoten parannellun menetelmän Windows-järjestelmien ja applikaatioiden hallintaan. (Lujan 2017.)

Vaikka aktiivihakemiston looginen rakenne on kaikkien käyttäjien, tietokoneiden ja muiden fyysisten resurssien hierarkkinen järjestelmä, metsä (forest) ja toimialueet (domain) muodostavat loogisen rakenteen perustan (kuva 4). Metsät, jotka ovat loogisen rakenteen turvallisuusrajoja, voidaan laatia tarjoamaan organisaation tiedon ja palvelujen itsenäisyyttä ja eristyneisyyttä tavalla, joka voi poistaa riippuvuudet fyysiseen topologiaan. Toimialueet metsän sisällä voidaan laatia tarjoamaan organisaation tiedon ja palvelujen yksinäisyyttä, mutta ei eristyneisyyttä. Loogisen ja fyysisen rakenteen erottaminen yksinkertaistaa ja vähentää hallinnan kustannuksia, koska muutokset fyysisessä rakenteessa eivät vaikuta loogiseen rakenteeseen. (Microsoft 2014.)



Kuva 4. Metsä ja siihen kuuluvat toimialueet.

Aktiivihakemistopalvelu asennetaan Windows Server -käyttöjärjestelmää ajavalle palvelimelle, joka on konfiguroitu toimimaan Domain Controllerina. Domain Controller on aktiivihakemiston sydän. Sen tehtävänä on pitää yllä aktiivihakemiston tietokantaa ja hoitaa toimialueen käyttäjien autentikointi. (Thomas 2016, 158.)

4.1 **Aktiivihakemiston työkalut**

Windows Server 2016:n mukana tulee monta sisäänrakennettua työkalua, joiden avulla on mahdollista hallita käyttöjärjestelmää. Thomasin (2016, 30) mukaan Windows Server 2016 on suunniteltu hallitavaksi etäältä mieluummin kuin paikallisesti. Esimerkkinä Thomas käyttää Windows Nano Server -käyttöönottovaihtoehtoa, missä vain yleisimpiä konfigurointeja voi suorittaa paikallisessa konsolissa. Jos halutaan tehdä jotakin haastavampaa, täytyy palvelimeen luoda etäyhteys esimerkiksi Windows PowerShellillä tai Remote Server Administration Tool (RSAT) -etähallintatyökalulla. Thomas kertoo tämän muutoksen johtuvan siitä, että nykyisin palvelimet ovat virtualisoituja ja harvoin sijaitsevat organisaation omissa tiloissa.

Vaikka samojen tehtävien suorittamiseen voi käyttää useita työkaluja, kuten Active Directory Administrative Center tai Server Manager -konsolia, Thomasin (2016, 30) mukaan Microsoftin järjestelmänhallinnan filosofiana on automatisoida kaikki toistuvat tehtävät Windows PowerShellillä. Suuressa organisaatiossa järjestelmänvalvoja hallitsee satoja tai tuhansia palvelimia, joiden hallitseminen manuaalisesti olisi mahdotonta. Tässä työssä salasanatiivisteiden hankkimiseen käytetään kolmea komentorivityökalua: Powershell, Ntdsutil ja Vssadmin.

Monet aktiivihakemiston hallintaan liittyvät tehtävät ovat useimmiten toistuvia. PowerShell on ensisijainen työkalu Microsoft-pohjaisten alustojen skriptaukseen, tehtävien automatisointiin ja hallintaan. PowerShell sisältää interaktiivisen kehotteen sekä skriptausympäristön, joita voidaan käyttää erikseen tai yhdessä. (Microsoft n.d.)

PowerShell on ollut oletuksena asennettuna kaikkiin Windows-käyttöjärjestelmiin Windows 7- ja Windows 2012 R2 -käyttöjärjestelmien julkaisusta lähtien vuodesta 2009. Vuonna 2016 Microsoft teki PowerShellistä avoimen lähdekoodin ohjelmiston sekä monialustaisen tarjoamalla yhteensopivuuden macOS-, CentOS- ja Ubuntu -käyttöjärjestelmien kanssa. (Microsoft n.d.)

Windows PowerShell esittelee cmdlet-konseptin, jossa yksinkertainen yhden funktion komento suorittaa useita muita funktioita. Cmdletejä voidaan käyttää suorittamaan yksittäisiä tehtäviä, ja yhdistelemällä useita cmdletejä voidaan suorittaa haastavia tehtäviä yksinkertaisemmin. PowerShellin mukana tulee yli sata ydin cmdletiä, ja kuka tahansa voi luoda omia cmdletejä ja jakaa niitä muiden käytettäväksi. (Microsoft n.d.)

Ntdsutil.exe on komentorivityökalu, joka tarjoaa hallintatoiminnot aktiivihakemiston Domain Services (AD DS) sekä Lightweight Directory Services (AD LDS) hallintaan. Ntdsutil-komennoilla voidaan suorittaa esimerkiksi AD DS:n tietokantojen ylläpitoa, prossien hallintaa ja valvontaa sekä huolimattomasti poistettujen ohjelmistojen ja laitteiden jäljelle jääneen metadatan poistamista. (Microsoft 2016.)

Tässä työssä käytetään Ntdsutil-työkalun komentoa IFM (Install From Media) salasanatiedostojen hakemiseen Domain Controller -koneelta. IFM-komentoa käytetään, kun halutaan luoda uusi Domain Controller ja siirtää siihen data aikaisemmasta Domain Controllerista. Tämä tapa on hyödyllinen, kun ei haluta tehdä normaalia aktiivihakemiston replikointia uuden Domain Controllerin asuttamiseen. (Clines & Loughry 2008, 297–298.)

Volume Shadow Copy Services (VSS) on teknologia, joka mahdollistaa palautuspisteen (snapshot) luomisen kovalevyllä olevasta datasta. VSS:n avulla voidaan luoda yhdenmukainen varmuuskopio käytössä olevasta tiedostosta, kuten tietokannasta. Windowsin muut varmuuskopiointipalvelut käyttävät VSS:ää varmistamaan, että varmuuskopioitu tieto on yhdenmukaista ja vastaa sitä tilaa, jossa tieto oli kun varmuuskopiointi aloitettiin, keskeyttämättä tiedoston käyttöä. (Thomas 2017, 706.)

Vssadmin on komentorivityökalu, jota käytetään VSS palautuspisteiden käsittelemiseen. Vssadminilla voidaan esimerkiksi luoda ja poistaa palautuspisteitä, määrittää niiden tallennussijainti ja tarkastella jo olemassa olevia palautuspisteitä. (Thomas 2017, 707.)

4.2 **Käyttäjätunnukset**

Tunnukset edustavat aktiivihakemistoympäristössä identiteettejä, jotka tietokonejärjestelmä tai verkko pystyy todentamaan. Yleisin tunnustyyppi aktiivihakemistossa on käyttäjätunnus, joka edustaa Windows-ympäristössä toimivaa käyttäjää. Käyttäjätunnukset edustavat aktiivihakemistoympäristössä lähes aina oikeita ihmisiä, sillä erotuksella, että jotkut tietokoneohjelmat käyttävät käyttäjätunnuksia erilaisten tehtävien suorittamiseen. (Thomas 2016, 173.)

Käyttäjätunnusten avulla käyttäjälle saadaan luotua identiteetti. Domain Controller pystyy käyttämään käyttäjätunnusta todentamaan pääsyn toimialueelle ja antamaan tälle valtuudet toimialueen resursseihin käyttäjätunnukselle annettujen oikeuksien mukaan. Käyttäjätunnukset luokitellaan usein ryhmiin esimerkiksi käyttäjän työnkuvan mukaan, ja resurssien käyttöoikeudet määritellään näille ryhmille. (Thomas 2016, 173.)

Käyttäjätunnukselle tulisi antaa pääsy vain niihin resursseihin, mitä tunnuksen käyttäjä tarvitsee työnsä suorittamiseen. Esimerkiksi markkinointiyksikössä työskentelevä henkilö ei tarvitse samoja oikeuksia kuin järjestelmänvalvoja. Tämä auttaa vähentämään hyökkäyspinta-alaa poistamalla turhat oikeudet, jotka saattavat johtaa tietoverkkoon murtautumiseen. Tätä konseptia kutsutaan nimellä Principle of least privilege. Jokaisessa käyttöjärjestelmässä on mahdollisuus määrittää, mihin resursseihin käyttäjätunnuksella on pääsy, yksityiskohtaisesti tai ryhmien perusteella. (Gibson 2015, 46.)

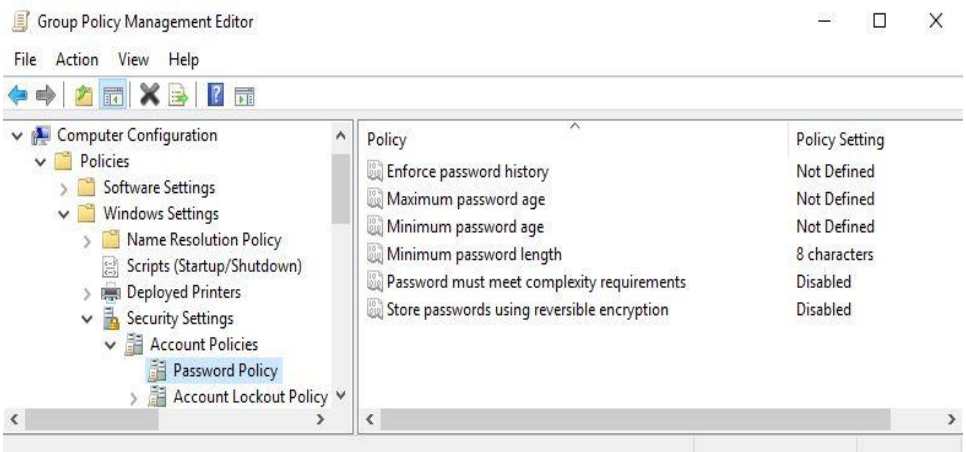
4.3 Ryhmäkäytännöt

Ryhmäkäytännöt tarjoavat sentralisoidun menetelmän aktiivihakemiston käyttäjien ja tietokoneiden hallintaan. Tämä tarkoittaa sitä, että asetukset voidaan ottaa käyttöön joko tietokone- tai käyttäjäkohtaisesti. Järjestelmänvalvoja voi ottaa setuksia käyttöön skenaariosta riippuen. Ryhmäkäytäntöjen avulla pystytään konfiguroimaan mitä vain: salasanakäytännöt, ohjelmistojen asentaminen, tietokoneen työpöydän asetuksen ja oletusohjelmistojen määritteleminen. (Thomas 2017, 182.)

Ryhmäkäytäntöjä voidaan ottaa käyttöön paikallisella tasolla, jolloin käytännöt vaikuttavat vain yksittäiseen laitteeseen. Ryhmäkäytännöt voidaan ottaa käyttöön myös aktiivihakemiston kautta, jolloin käytännöt vaikuttavat toimialueeseen yhdistettyihin laitteisiin tai käyttäjiin. (Thomas 2017, 182.)

Ryhmäkäytäntöasetukset konfiguroidaan ja talletetaan Group Policy Objectin (GPO) sisällä. Paikallisia ryhmäkäytäntöobjekteja voidaan muokata kohdekoneella Local Group Policy Editor (LGPO) -työkalun avulla. Windows Server -ympäristössä toimialueen laitteita koskevia ryhmäkäytäntöjä hallitaan Group Policy Management -konsolin (GPMC) avulla. (Arya 2016, 2.)

Monet organisaatiot ottavat käyttöön salasanakäytännöt, jotka tarjoavat käyttäjille salasanasäännöt. Käytäntö määrittää salasanan minimivaatimukset. Järjestelmänvalvojat voivat pakottaa salasanakäytännön kaikille toimialueen käyttäjille käyttämällä esimerkiksi aktiivihakemiston ryhmäkäytäntöjä. Kuvassa 5 on esitettynä salasanakäytännöt hallintokonsolissa. (Gibson 2015, 67.)



Kuva 5. Windows-aktiivihakemiston salasanakäytännöt.

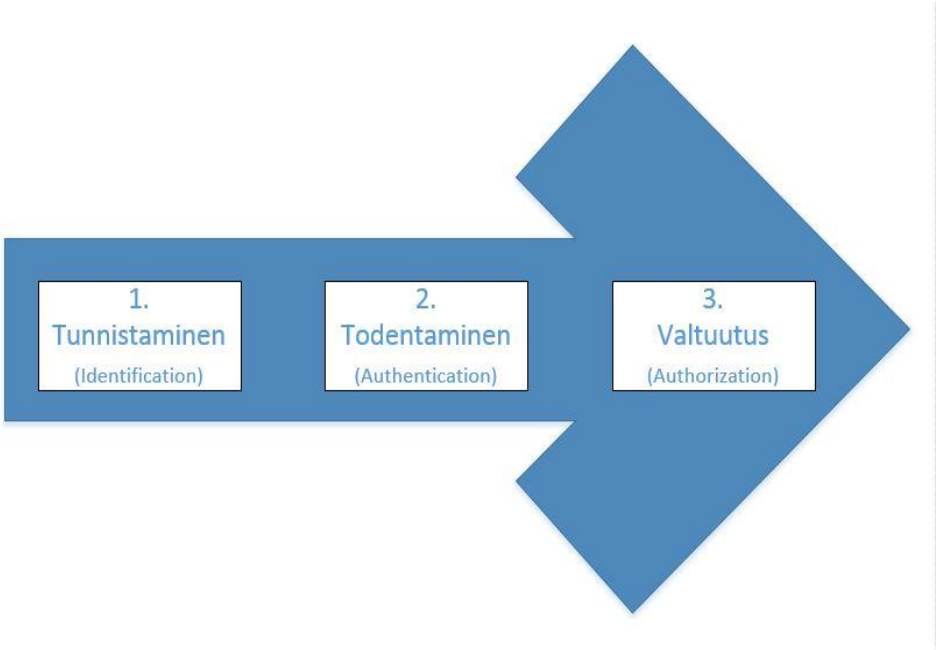
Enforce password history -käytäntö määrittää, kuinka monta aikaisempaa käyttäjän salasanaa järjestelmä muistaa ja estää näiden salasanojen uudelleenkäyttämisen. Maximum ja Minimum password age -käytännöt määrittävät, kuinka kauan salasana saa olla käytössä ennen kuin se täytyy vaihtaa uuteen ja kuinka kauan salasanan pitää olla ollut käytössä ennen kuin sen voi vaihtaa uuteen. Minimum password length -käytäntö määrittää, kuinka monta merkkiä pitkä salasanan tulee vähintään olla. Kun Password must meet complexity requirements -käytäntö on otettuna käyttöön, salasanan täytyy sisältää kolme tai neljä eri merkkityyppiä, kuten suuret kirjaimet, pienet kirjaimet, numerot ja erikoismerkit. (Gibson 2015, 68.)

Tässä työssä salasanakäytännössä käytetään NISTin uusia ohjenuoria. Käyttäjälle ei anneta muita vaatimuksia kuin että salasanan minimipituus on 8 merkkiä.

4.4 **Pääsynhallinta**

Keskeisin osa mitä tahansa pääsynhallintajärjestelmää on käyttäjien tunnistaminen ja todennus. Jos käyttäjiä ei voida tunnistaa, käyttäjät ovat todentamattomissa, eikä heidän pääsyä erinäisiin resursseihin pystytä määrittämään. Tällöin pääsy resursseihin on joko kaikilla tai ei kenelläkään. Käyttäjät voidaan tunnistaa esimerkiksi käyttäjätunnusten avulla. (Gibson 2015, 62.)

Kuvassa 6 on esitettynä tunnistamisen, todentamisen ja valtuuttamisen prosessi. Ensimmäisenä käyttäjä tunnustaa identiteetin esimerkiksi käyttäjätunnuksella ja seuraavaksi todentaa identiteetin antamalla todennustiedot, kuten salasanan. Kolmantena pääsynhallintajärjestelmä tarkistaa annetut kirjautumistiedot ja valtuuttaa käyttäjälle pääsyn resursseihin, kuten palvelimella sijaitseviin tiedostoihin. Jos nämä kolme askelta eivät toteudu, käyttäjä ei pääse käsiksi pääsynhallintajärjestelmällä suojattuihin resursseihin. (Gibson 2015, 62.)



Kuva 6. Tunnistaminen, todentaminen ja valtuutus.

Windows aktiivihakemistossa oletustodennusprotokolla on symmetrisesti salattuun lippujärjestelmään perustuva Kerberos. Kerberos on suunniteltu tarjoamaan vahva todentaminen toimialueympäristöissä. (Gordon 2015, 873.)

Kerberoksen todennusprosessi perustuu kommunikointiin kolmen järjestelmän välillä: pyytävä järjestelmä eli asiakas, palvelin missä resurssit sijaitsevat ja Kerberos/Key Distribution Center (KDC). Asiakas on mikä tahansa entiteetti, kuten käyttäjä työpisteellä, applikaatio tai sovellus, joka kommunikoi Kerberos-palvelimen kanssa. KDC tarjoaa kaksi funktiota todennusprosessiin – se toimii todennuspalvelimena (authentication server, AS) ja lippupalvelimena (ticket-granting server, TGS). Näiden avulla KDC todentaa asiakkaan ja myöntää asiakkaalle palvelulippuja, joiden avulla todennus tapahtuu. (Gordon 2015, 873.)

Kerberos on esimerkki kertakirjautumisjärjestelmästä hajautetussa verkkoympäristössä. Kertakirjautumisella, englanniksi single sign-on (SSO), käyttäjän tarvitsee tunnistautua vain kerran koko istunnon aikana käyttäessään organisaation, tai luotetun yhteistyökumppanin, resursseja. Tämä parantaa tietoturvaa, koska käyttäjien tarvitsee muistaa vain yhdet kirjautumistunnukset, jolloin tunnusten kirjoittaminen esimerkiksi muistilapulle on vähemmän todennäköistä. Kertakirjautumisen haittapuolena on se, että jos hyökkääjä saa tunnukset käsiinsä, hän pääsee käsiksi kaikkiin käyttäjän saatavilla oleviin resursseihin kaikkialla organisaatiossa. (Gibson 2015, 76.)

Toimiakseen Kerberos vaatii, että järjestelmät ovat yhteensopivia ja osana toimialuetta. Jos Kerberosta ei ole mahdollista käyttää tietojärjestelmäympäristössä, oletustodennusprotokollaksi otetaan NTLMv2. (EC-Council 2010, 5-12.)

New Technology LAN Manager (NTLM) -protokollaperhe on useiden Microsoft tuotteiden käyttämä todennusprotokolla, jota käytetään toteuttamaan haaste-vaste -todennus (challenge-response) Windows-ympäristössä. NTLM-todennusprotokollaa käyttäessä käyttäjän salasanaa ei lähetetä verrattavaksi, vaan autentikointipalvelin lähettää haasteen asiakasjärjestelmälle. Asiakasjärjestelmä lähettää todennuspalvelimelle vastauksen, joka on funktio haasteeseen, eli käyttäjän salasanan ja mahdollisesti muuta tietoa. Oikean vastauksen laskemiseen tarvitaan käyttäjän oikea salasana. (EC-Council 2010, 5-11.)

NTLM-protokollaperheeseen kuuluu LAN Manager (LM) versiot 1 ja 2, sekä NTLM versiot 1 ja 2. Molemmat LM versiot sekä NTLMv1 on tutkittu ja todettu heikoiksi. Tämän takia vain NTLMv2-protokollan käyttäminen on suositeltavaa. (EC-Council 2010, 5-13.) Taulukossa 1 on esitettynä NTLM-protokollaperheen todennusalgoritmien eroavaisuudet.

Taulukko 1. NTLM-protokollaperheen todennusalgoritmien eroavaisuudet. (EC-Council 2010, 5-12.)

	LM	**NTLMv1**	**NTLMv2**
Isot ja pienet kirjaimet	Ei	Kyllä	Kyllä
Tiivistealgoritmi	DES (ECB moodi)	MD4 (NT-tiiviste)	MD4 (NT-tiiviste)
Haaste-vaste -algoritmi	DES (ECB moodi)	DES (ECB moodi)	HMAC-MD5

4.5 Salasanat aktiivihakemistossa

Sekä paikalliset että toimialueen salasanat varastoidaan aktiivihakemiston tietokantaan. Aktiivihakemisto varastoi tietokantaansa jokaisessa Domain Controllerissa NTDS.dit -tiedostossa. NTDS.dit-tiedostossa salasanoja ei säilytetä selkotekstimuodossa vaan salasanat on salattu tiivistealgoritmilla. Salasanojen tiivistäminen voidaan toteuttaa kahdella eri algoritmilla, LM (LAN Manager) ja NT. NT-tiivistettä kutsutaan usein myös NTLM-tiivisteeksi. Useimmiten sekä LM- että NTLM-tiivistettä säilytetään NTDS.dit -tiedostossa.

LAN Manager (LM) tiivisteet ovat peräisin käyttäjien salasanoista. LM-tiivistettä käytetään vanhemmissa laitteistossa ja Microsoftin turvallisuusohjeet ovat suositelleet LM-tiivisteen käyttämisestä luopumista jo vuosikymmenien ajan. LM-tiivisteissä on useita ominaispiirteitä, jotka tekevät

niistä vähemmän turvallisia. Salasanan täytyy olla alle 15 merkkiä pitkä, eikä se saa sisältää muita kuin ASCII-merkkejä. LM-tiivisteet eivät erottele suuria eikä pieniä kirjaimia, vaan muuttaa salasanan kaikki merkit isoiksi kirjaimiksi. LM-tiivisteiden purkaminen vaatii erittäin vähän vaivaa ja tapoja niiden purkamiseen on ollut saatavilla useita vuosia. (Jungles ym. 2012, 35.)

Salasanan NTLM-tiiviste lasketaan käyttämällä MD4-tiivistealgoritmia. MD4 on kryptografinen yksisuuntainen funktio, joka luo salasanasta matemaattisen esitysmuodon. NTLM-tiiviste on suunniteltu luomaan aina sama tiiviste samasta salasanasta, joka minimoi törmäykset (collision). Tiivisteistä puhuttaessa törmäys tarkoittaa, että kaksi eri salasanaa tuottavat saman tiivisteen. NTLM-tiiviste on aina pituudeltaan tietyn pituinen, eikä tiivistettä pysty suoraan purkamaan takaisin selkotekstiksi. Kumpaakaan, LM tai NTLM-tiivistettä, ei ole suolattu, mikä helpottaa niiden murtamista huomattavasti. (Jungles ym. 2012, 35.)

NTDS.dit-tiedosto on salattu SYSTEM-rekisteritiedostossa sijaitsevalla Syskey-apuohjelmalla tietoturvan parantamiseksi. Syskey on Windowsin sisäinen juuritason salausavain, jota käytetään salaamaan arkaluonteiset käyttöjärjestelmätiedostot, kuten käyttäjien ja salasanojen tiivisteet, 128-bittisellä Rivest Cipher 4 (RC4) -salausalgoritmilla. (EC-Council 2010, 5-18.) Taulukossa 2 on esitetty salasanatiivisteiden hankkimiseen tarvittavien tiedostojen oletussijainnit.

Taulukko 2. NTDS.dit ja SYSTEM tiedostojen oletussijainnit.

Oletuspolku	**Kuvaus**
C:\Windows\NTDS\ntds.dit	Aktiivihakemiston tietokanta
C:\Windows\System32\config\SYSTEM	Rekisteritiedosto, joka sisältää tiivisteiden salaamiseen käytettävän avaimen

5 SALASANA-AUDITOINTI

Salasana-auditointi toteutetaan Windows Server 2016 -palvelinkäyttöjärjestelmäympäristöön luotujen testikäyttäjien salasanoilla. Palvelimelle on asennettu aktiivihakemistopalvelu ja palvelin on korotettu domain controlleriksi. Testiympäristössä on muokattu salasanakäytäntöjä ryhmäkäytäntöjen avulla mukailemaan NISTin uusia suosituksia, eli salasanalla ei ole muita vaatimuksia kuin että se on vähintään 8 merkkiä pitkä. Testikäyttäjiä tässä ympäristössä on noin kaksisataa, ja heille on luotu sekä vahvoja että heikkoja salasanoja. Salasanojen purkaminen toteutetaan työpöytäkäyttöön tarkoitetulla tietokoneella, jonka komponentit on esitetty taulukossa 3.

Taulukko 3. Salasanojen purkamiseen käytetyn tietokoneen komponentit.

Komponentti	Kuvaus
Näytönohjain	NVIDIA GeForce GTX 1060 6GB
Prosessori	Intel Core i7 4770K @ 3.50GHz

5.1 Salasanatiivisteiden hankkiminen

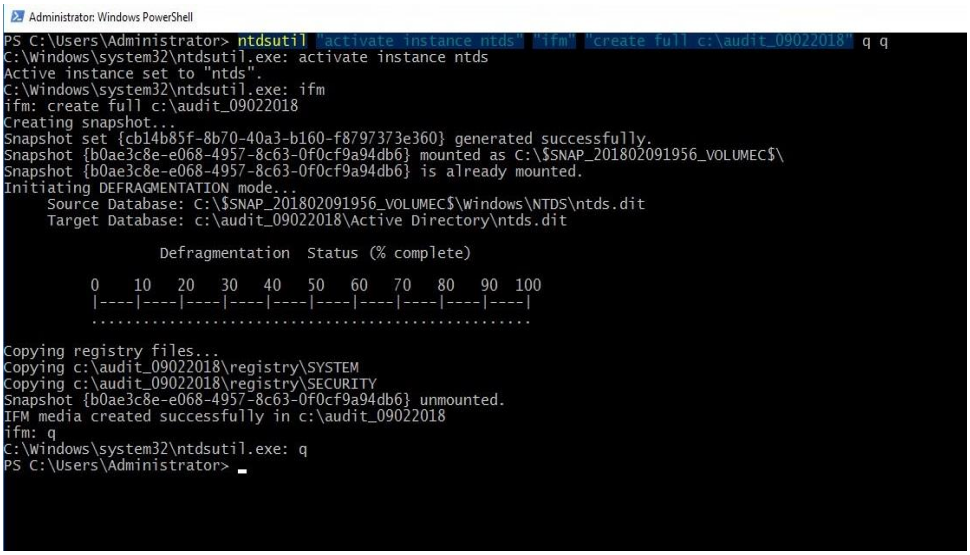
Salasanojen tiivisteiden käsiin saamiseksi NTDS.dit-tiedostosta täytyy luoda kopio. Koska NTDS.dit tiedosto on jatkuvasti aktiivihakemiston käytössä, se on lukittu kopioinnilta ja avaamiselta, jonka takia normaali tiedoston kopioiminen ei onnistu. Tiedoston kopioimiseen voidaan käyttää Ntdsutil-diagnosointityökalua tai Vssadmin-komentorivityökalua.

5.1.1 Ntdsutil-työkalulla

VSS-palautuspiste NTDS.dit-tiedostosta voidaan luoda helposti Ntdsutil-diagnosointityökalulla. Ntdsutil-työkalu käynnistetään domain controller -koneella järjestelmänvalvojana avatussa PowerShell-komentokehotteessa kirjoittamalla komento *ntdsutil ”activate instance ntds” ”ifm” “create full c:\audit_09022018” q q*. Tällä tavoin kaikki komennot voidaan suorittaa automatisoidusti. Komennot voidaan suorittaa myös tavallisella komentorivillä, jolloin jokainen komento täytyy syöttää manuaalisesti.

PowerShell avataan järjestelmänvalvojana klikkaamalla komentokehotetta hiiren oikealla näppäimellä ja valitsemalla ”Suorita järjestelmänvalvojana”. Aktiivihakemisto valitaan aktiiviseksi instanssiksi komennolla *active instance ntds*. Yksi tapa NTDS.dit tiedoston lukituksen kiertämiseen on luoda kopio Domain Controllerin asennusmediasta. Tämä tehdään Ntdsutil-työkalun alikomennolla *ifm*. Ifm:n käyttö vaatii, että aktiivinen in-

stanssi on valittuna. Komennolla *create full tiedostopolku* luodaan VSS palautuspiste domain controller asennusmediasta haluttuun kansioon. Ifm-alikomennosta ja ntdsutil-työkalusta poistutaan peräkkäisillä quit, ”q”, komennoilla. Kuvassa 7 on esitetty NTDS.dit- ja SYSTEM-tiedostojen kopiointi Ntdsutil-työkalulla.



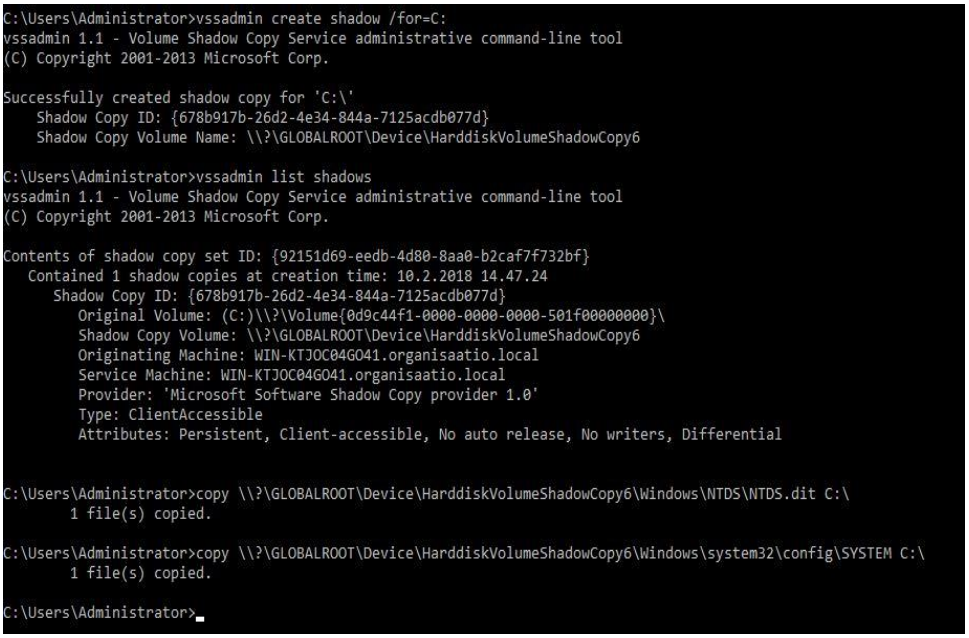
Kuva 7. NTDS.dit- ja SYSTEM-tiedostojen kopiointi Ntdsutil-työkalulla.

5.1.2 **Vssadmin-työkalulla**

NTDS.dit ja SYSTEM tiedostojen kopiointi onnistuu myös Vssadmin-työkalulla. Ensimmäisenä Vssadminilla luodaan tilannevedos C:\-aseman tiedostoista, mikä onnistuu järjestelmänvalvojana avatussa komentorivissä komennolla *create shadow /for=C:*.

Komento tulostaa onnistuneen tilannevedoksen luomisen jälkeen tilannevedoksen tunnusmerkkijonon sekä nimen. Kaikki luodut tilannevedokset voidaan listata komennolla *vssadmin list shadows*.

C:\-aseman tilannevedoksen luonnin jälkeen voidaan tilannevedoksesta kopioida NTDS.dit- sekä SYSTEM-tiedosto ja siirtää nämä tietokoneelle, jolla salasanojen murtaminen suoritetaan. Kuvassa 8 on esitettynä koko tilannevedoksen luomisprosessi sekä haluttujen tiedostojen kopioiminen. Tiedostoja kopioidessa tulee kiinnittää huomiota siihen, että tiedostot kopioidaan viimeisimmästä tilannevedoksesta. Tilannevedokset tallennetaan käyttäen juoksevaa numeroa, joka lisätään tilannevedoksen nimen perään.



Kuva 8. Tiedostojen kopiointi Vssadmin-työkalulla.

Domain Controller -koneella ei useimmiten haluta säilyttää turhia tiedostoja ja kopioita, joten ylimääräiset tilannevedokset tulisi poistaa. Tilannevedos voidaan poistaa komennolla *vssadmin delete shadows /shadow={Shadow Copy ID}*.

5.2 **Salasanatiivisteiden purkaminen**

Koska NTDS.dit sisältää muutakin tietoa kuin käyttäjien salasanojen NTLM-tiivisteet, täytyy tiivisteet purkaa erilliseen tiedostoon. Tähän on olemassa lukuisia työkaluja, mutta tässä työssä tähän käytetään Dionachin julkaisemaa NtdsAudit-työkalua. (Dionach 2018.)

Tiivisteiden purkaminen NtdsAudit-työkalulla onnistuu syöttämällä seuraava komento komentoriville: *NtdsAudit.exe "C:\ntds.dit" -s "C:\SYSTEM" -p tiivisteet.txt*. Komennossa käynnistetään NtdsAudit-työkalu, määritetään NTDS.dit-tiedoston sijainti, -s -argumentilla määritetään SYSTEM-tiedoston sijainti, -p -argumentilla käytetään SYSTEM-tiedostossa olevaa avainta purkamaan NTDS.dit-tiedoston salaus ja NTLM-tiivisteet puretaan tiivisteet.txt -nimiseen tekstitiedostoon. Kuvassa 9 on esitettynä tekstitiedoston sisältö. Tekstitiedostossa jokaisen käyttäjän tiedot esitetään omalla rivillään, ja käyttäjätunnuksen ominaisuudet on jaoteltu kaksoispisteellä eri osioihin.

```
organisaatio.local\Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:9A0198B452271B12ED7BFA3857896DE6::
organisaatio.local\Guest:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0::
organisaatio.local\DefaultAccount:503:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0:
organisaatio.local\krbtgt:502:AAD3B435B51404EEAAD3B435B51404EE:363D3C090531F26DB68E93F3CBD4EE0F::
organisaatio.local\jsmith:1103:AAD3B435B51404EEAAD3B435B51404EE:64F12CDDAA88057E06A81B54E73B949B::
organisaatio.local\psalo:1104:AAD3B435B51404EEAAD3B435B51404EE:F23A5B5B7ED9ADEE35713B864D2F9A2A::
organisaatio.local\lhume:1105:AAD3B435B51404EEAAD3B435B51404EE:259745CB123A52AA2E693AAACCA2DB52::
organisaatio.local\aeaston:1107:AAD3B435B51404EEAAD3B435B51404EE:46BA1790939CB60F3EADF0CD5CD77015::
organisaatio.local\dpound:1108:AAD3B435B51404EEAAD3B435B51404EE:D4C35D6A524AEC7024BD92D7ACC372D2::
organisaatio.local\ktimberlake:1109:AAD3B435B51404EEAAD3B435B51404EE:E00300DACDC07C27246D64773DBB32A3::
organisaatio.local\jkuittinen:1110:AAD3B435B51404EEAAD3B435B51404EE:B7D6F9A2589C11C3E3C755A8333EFA1C::
```

Kuva 9. Toimialueen käyttäjien salasanatiivisteet.

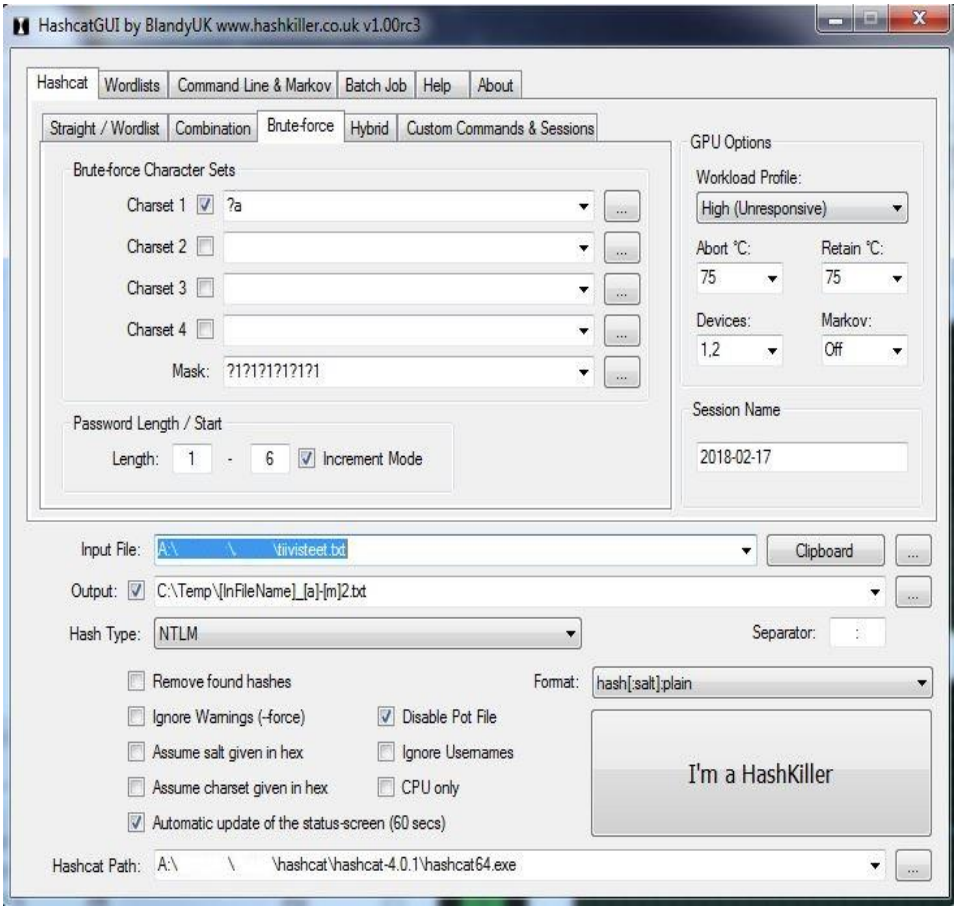
Ensimmäisenä on esitetty toimialueen nimi sekä käyttäjätunnus. Seuraava osio sisältää käyttäjän tunnusnumeron. Kolmannessa osiossa on salasana tiivistettynä LM-formaattiin. Kuten kuvassa 9 näkyy, kaikilla käyttäjillä on sama LM-tiiviste ”AAD3B435B51404EEAAD3B435B51404EE”. Tämä tarkoittaa LM-kielellä tyhjää arvoa. Oletuksena NTDS.dit-tiedostoon tallennetaan sekä LM-tiiviste, että NTLM-tiiviste, vaikka LM-tiivisteitä ei käytettäisikään. NTLM-tiivisteet ovat esitettynä neljännessä osiossa LM-tiivisteiden jälkeen.

5.3 **Salasanojen murtaminen erilaisilla menetelmillä**

5.3.1 **Brute force -menetelmä**

Brute force -menetelmä voidaan toteuttaa esimerkiksi käyttämällä Hashcat nimistä työkalua. Hashcat hyödyntää salasanojen murtamiseen pääosin näytönohjaimia, mutta myös pelkkää prosessoria voidaan käyttää murtamiseen. Hashcat on komentorivityökalu, mutta siihen on saatavilla myös HashcatGUI-lisäosa, joka luo työkalulle graafisen käyttöliittymän. Kuvassa 10 on esitettynä HashcatGUI Brute force -käyttöliittymä. Käyttöliittymässä voidaan asettaa brute force -menetelmälle useita sääntöjä.

Brute-force Character Sets -osiossa voidaan määritellä tiettyjä merkistöjä, esimerkiksi määrittämään sisältyykö salasanaan erikoismerkkejä tai numeroita. Merkistöt ja Hashcatin lyhenteet merkistöille on esitettynä taulukossa 4. Tässä työssä brute forcetaan kaikki mahdolliset 1-7 merkkiä pitkät salasanat, jotka sisältävät isoja ja pieniä kirjaimia, numeroita sekä erikoismerkkejä. Jotta näytönohjaimet eivät vaurioituisi, näytönohjaimien kuormitusta ja turvarajoja voi asettaa GPU Options -osiossa. Tiivisteet, jotka halutaan murtaa, lisätään liittämällä tiivistetiedoston tiedostopolku Input File -kohtaan. Viimeisenä valitaan tiivistetyyppi, joka halutaan murtaa. Tässä työssä murretaan NTLM-tiivisteitä, joten tiivistetyyppi on NTLM. Murtaminen saadaan aloitettua painamalla I’m a HashKiller -painiketta. Hashcat aukeaa komentorivi-ikkunaan, josta voi tarkkailla murtamisen etenemistä.



Kuva 10. Hashcatin graafinen käyttöliittymä.

Taulukko 4. Hashcat merkistöjen lyhenteet.

Lyhenne	Merkistö
?l	abcdefghijklmnopqrstuvwxyz
?u	ABCDEFGHIJKLMNOPQRSTUVWXYZ
?d	0123456789
?s	!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
?a	Kaikki edelliset (?l?u?d?s)

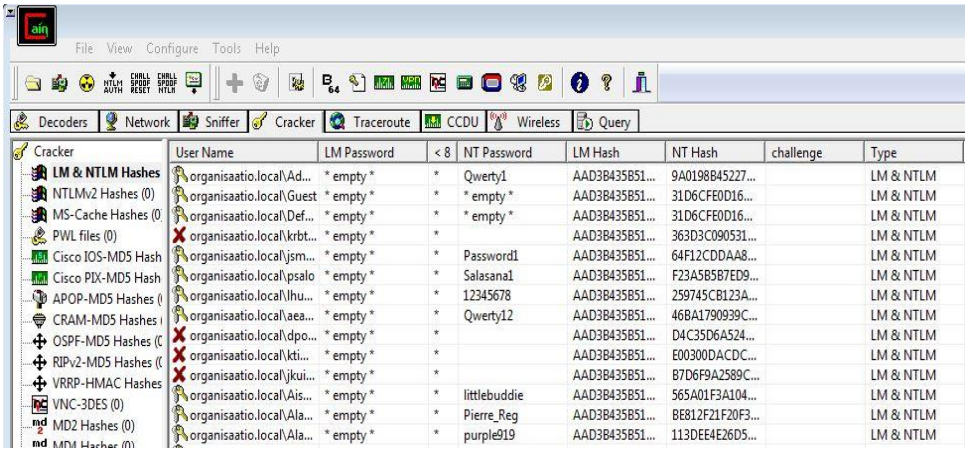
Murretut salasanat tulostuvat määritettyyn Output-tiedostoon tiiviste-selkoteksti -formaatissa.

5.3.2 **Sanakirja-menetelmä**

Sanakirja-menetelmä vaatii valmiita mahdollisia salasanoja sisältäviä sanalistoja toimiakseen. Sanalistoja löytyy ilmaisena ladattavana esimerkiksi Skullsecurityn wiki-sivustolta. (Skullsecurity n.d.)

Työssä käytetään sanakirja-menetelmän suorittamiseen Cain & Abel -työkalua. Cain ei käytä murtamiseen näytönohjaimen laskentatehoja vaan

pelkkää prosessorin suoritintehoa. Työkalu sisältää lukuisia määriä erilaisia tietoturvaan ja testaukseen liittyviä ominaisuuksia. Cracker-välilehti sisältää kaiken mikä liittyy salasanojen murtamiseen. Cain & Abelin käyttöliittymä salasanojen murtamiseen on esitettynä kuvassa 11.

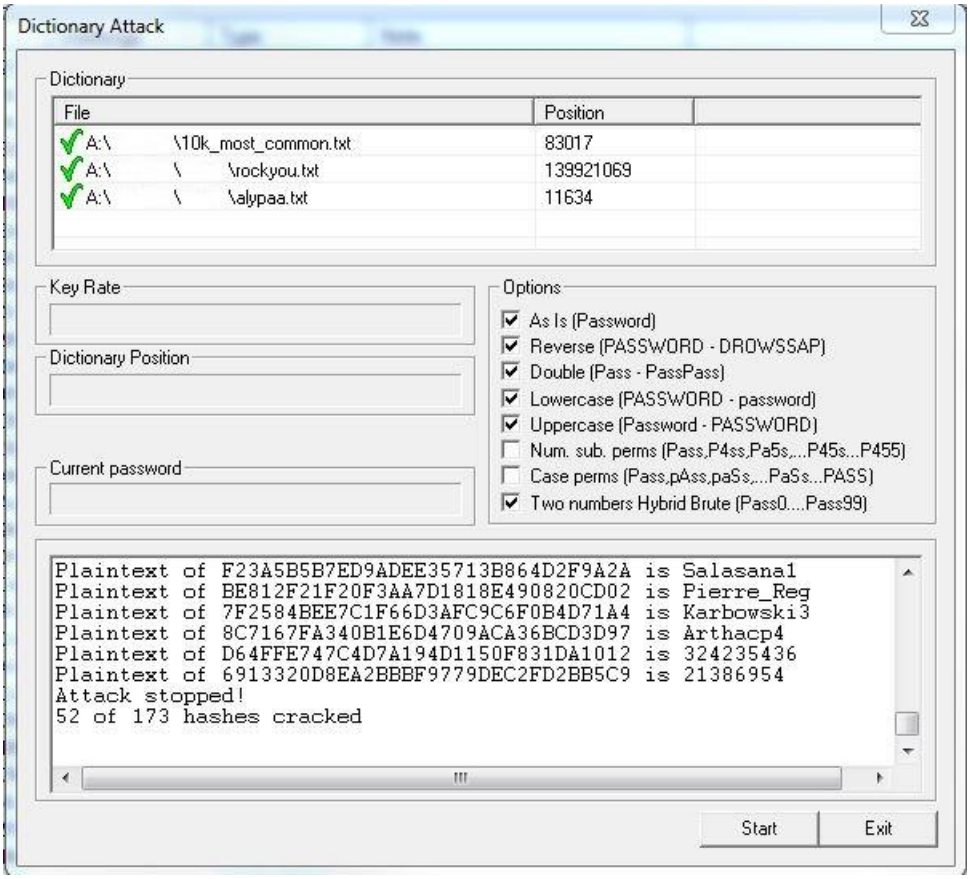


Kuva 11. Cain & Abel käyttöliittymä salasanojen murtamiseen.

NTLM-tiivisteet sisältävä tiedosto lisätään murrettavaksi avaamalla ensin LM & NTLM Hashes -ikkuna aktiiviseksi. Tiivisteet lisätään klikkaamalla tyhjää LM & NTLM Hashes -ikkunaa hiiren oikealla painikkeella ja valitsemalla Add to list tai klikkaamalla työkalurivissä olevaa plus-symbolia. Murrettavaksi voidaan tuoda tiivisteet paikallisesta järjestelmästä valitsemalla Import Hashes from local system. Tässä työssä auditoidaan kuitenkin aktiivihakemistosta saatuja tiivisteitä, mikä onnistuu tuomalla tiivistetiedosto valitsemalla Import Hashes from a text file.

Tiivistetiedoston lisäämisen jälkeen tiivisteitä voidaan valita yksittäin tai joukossa murrettavaksi. Helpoin tapa valikoida kaikki tiivisteet murrettavaksi kerralla on klikata ikkunaa hiiren oikealla näppäimellä ja valita pikavalikosta Select all. Tiivisteiden valikoinnin jälkeen pikavalikosta valitaan Dictionary Attack ja NTLM hashes, mikä avaa Dictionary Attack ikkunan (kuva 12). Dictionary Attack -ikkunassa sanalistat, joita halutaan käyttää, lisätään File-ikkunaan valitsemalla pikavalikosta Add to list. Sanalistojen lisäämisen jälkeen sanakirja-menetelmä voidaan aloittaa painamalla Start-painiketta.

Cainilla sanakirja-menetelmää voidaan muokata helposti hyödyntämään erilaisia ominaisuuksia. Sanalistaa voidaan verrata tiivisteisiin sellaisenaan tai sanalistan sanoja voidaan muokata esimerkiksi muuttamalla sanojen kirjainten ja merkkien paikkoja keskenään tai kääntämällä sana väärin päin. Kuvassa 12 on esitettynä suoritettu salasanojen murtamisprosessi Cain & Abel -työkalulla sekä saatavilla olevat sanalistan muokkausominaisuudet.



Kuva 12. Suoritettu salasanojen murtaminen sanakirja-menetelmällä.

5.3.3 **Rainbow table -menetelmä**

Rainbow table -menetelmän suorittamiseksi tässä työssä käytetään ilmaista Ophcrack-ohjelmistoa. Ophcrackin mukana tulee useita ilmaisia LM- sekä NTLM-tiivisteiden purkamiseen tarkoitettuja rainbow tableja. Rainbow tablet saa ladattua Ophcrackin verkkosivustolta. Tässä työssä käytetään 8 gigatavun kokoista Vista special -rainbow tablea, mikä pitää sisällään salasanojen tiivisteitä, jotka ovat maksimissaan 8 merkkiä pitkiä.

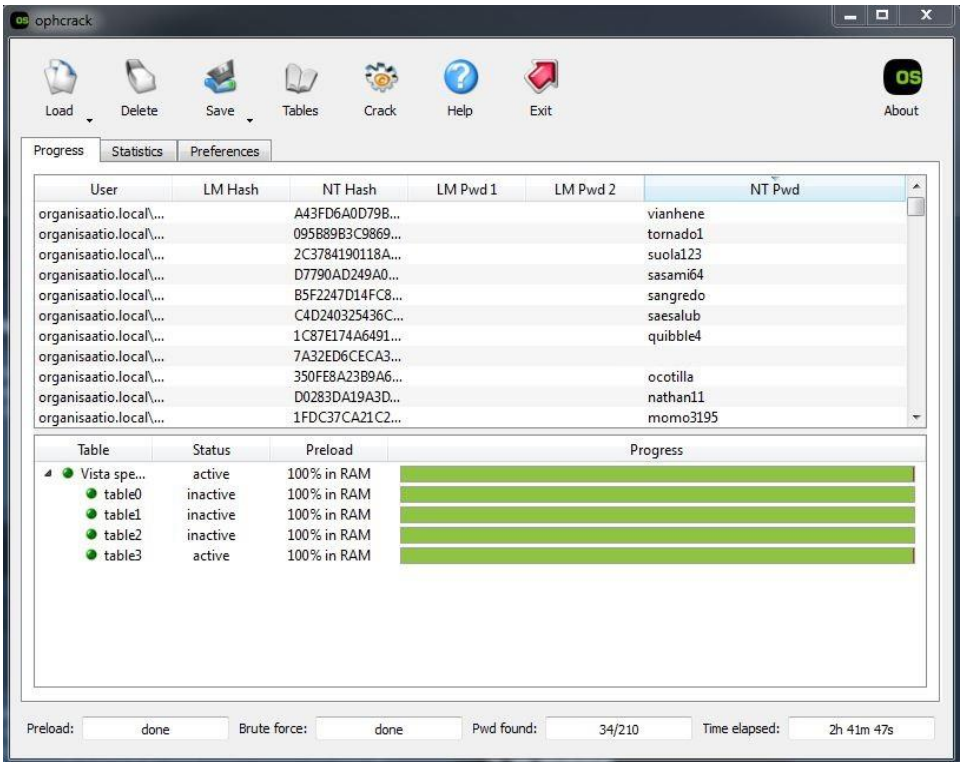
Ensimmäisenä Ophcrackissa on hyvä konfiguroida asetukset. Preference-välilehdessä voi määrittää esimerkiksi, kuinka montaa prosessorin ydintä salasanojen murtamiseen käytetään. Välilehdessä on mahdollista myös laittaa päälle auditointimoodi. Auditointimoodissa käyttäjien nimet piilotetaan sekä sen sijaan että murrettujen salasanojen selkotekstit näytettäisiin, Ophcrack kertoo vain sen, onko salasanaa murrettu vai ei. Asetusten muuttamisen jälkeen Ophcrack tulee käynnistää uudelleen muutosten voimaan tulemiseksi.

Rainbow tablet ladataan Ophcrackissa valitsemalla Tables, mikä avaa Table Selection -hallintaikkunan. Painamalla Install-painiketta auenneessa hallin-

taikkunassa ja valitsemalla kansio, mihin rainbow tablet on ladattu, rainbow table saadaan osoitettua Ophcrackin käyttöön. Table Selection -ikkunassa ladattujen rainbow tablejen tilaa voidaan muuttaa aktiiviseksi tai ottaa pois käytöstä.

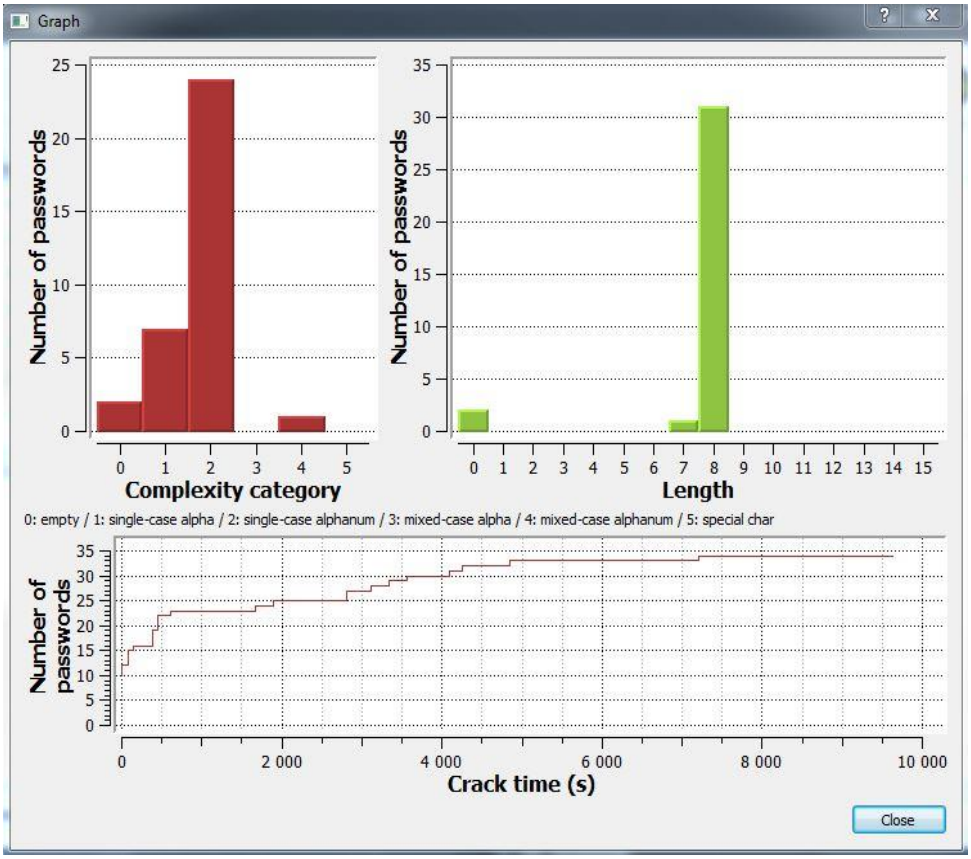
NTLM-tiivisteet lisätään Ophcrackiin Load-pudotusvalikosta valitsemalla PWDUMP file, koska NTLM-tiivisteet on purettu tekstitiedostoon. Ophcrackissa on myös mahdollista purkaa SAM-tiedosto suoraan SYSTEM-tiedoston avaimella tai valita yksittäinen tiiviste murrettavaksi.

Kun tiivisteet ja rainbow tablet on ladattu, murtaminen aloitetaan klikkaamalla Crack-painiketta. Murtamisen etenemistä voidaan tarkkailla Statistics-välilehdellä. Kuvassa 13 on esitettynä suoritettu rainbow table -menetelmä Ophcrack-ohjelmistolla.



Kuva 13. Suoritettu rainbow table -menetelmä Ophcrack-ohjelmistolla.

Ophcrack osaa tuottaa myös graafeja murretuista salasanoista ja niiden ominaisuuksista. Graafit saa näkyviin Statistics-välilehdellä valitsemalla Display graphs. Graafeista nähdään, kuinka kauan salasanojen murtamiseen kului aikaa, salasanojen pituus sekä monimutkaisuus. Monimutkaisuuskategoriat määräytyvät esimerkiksi sen mukaan, sisältääkö salasana erikoismerkkejä vai pelkkiä pieniä kirjaimia. Ophcrackin tuottamat graafit suoritetusta salasanojen murtamisesta on esitetty kuvassa 14.



Kuva 14. Ophcrack-ohjelmiston tuottama graafi puretuista salasanoista.

6 YHTEENVETO

Opinnäytetyössä selvitettiin, miten Windows-aktiivihakemistossa säilytetään salasanoja. Tämän jälkeen tutkittiin, miten salasanatiivisteet sisältävä tietokanta saadaan kopioitua salasanojen murtamista varten. Salasanatiivisteitä murrettiin käyttämällä brute force-, sanakirja- ja rainbow table -menetelmiä. Tutkimuskysymyksiin saatiin vastaukset aiheeseen liittyvää teoriaa tutkimalla sekä suorittamalla salasanojen murtaminen käytännössä. Tuloksena työssä luotiin ohje salasanatiedostojen hankkimiseen sekä salasanatiivisteiden murtamiseen käyttäen eri ohjelmistoja.

Brute force -menetelmän käyttäminen yli 8 merkkiä pitkien salasanojen auditoimiseen ilman yksinomaan salasanojen murtamiseen suunniteltua järjestelmää ei ole kannattavaa. Brute force -menetelmä on hyvä auditoimaan, ettei järjestelmästä löydy alle 7 merkkiä pitkiä salasanoja.

Sanakirja-menetelmän menestys riippuu täysin käytössä olevista sanalistoista. Organisaation olisi hyvä luoda omia sanalistoja sanoista, jotka esiintyvät organisaation nettisivuilla sekä työntekijöidensä sosiaalisen median profiileissa. Tarkoituksena on saada simuloitua metodeja, joita hyökkääjät käyttävät sanalistojen luomiseen.

Rainbow table -menetelmä on tehokas tapa murtaa salasanoja, mutta moderneilla laitteistoilla pystytään toteuttamaan lähes yhtä tehokas ja nopea murtaminen esimerkiksi brute force -menetelmällä. Rainbow tablet, jotka kattavat NTLM-tiivisteet 1-8 merkkiä pitkille salasanoille, voidaan helpommin korvata brute force -menetelmällä ilman tarvetta satojen gigatavujen suuruisille rainbow table -tietokannoille. Rainbow table -menetelmän epäkäytännöllisyyttä lisää se, että suuria, valmiiksi laskettuja ja ilmaisia rainbow tableja ei ole helposti saatavilla verkon kautta.

NISTin uusien salasanasuositusten ehdottama 8 merkin minimipituus on mielestäni liian lyhyt. Opinnäytetyötä tehdessä selvisi, että kaikki mahdolliset 8 merkkiä pitkät salasanat voidaan murtaa alle vuorokaudessa käyttäen moderneja näytönohjaimia. Tämän takia salasanojen minimipituuden tulisi olla esimerkiksi viestintäviraston ehdottama 15 merkkiä.

Organisaatioiden tulisi myös pohtia salasanojen hallintaohjelmien käyttämistä. Hallintaohjelmien avulla käyttäjille voitaisiin luoda erittäin vahvoja salasanoja ilman, että käyttäjien tarvitsee muistaa niitä ulkoa. Myös salasanojen vertaamista saatavilla oleviin yleisistä salasanoista koostuviin sanalistoihin salasanan luomisvaiheessa tulisi miettiä. Tällä tavoin heikkojen salasanojen luontia voitaisiin ennaltaehkäistä.

Opinnäytetyön aikana tutustuin ja opin paljon Windows Server 2016:n järjestelmistä, kuten siitä miten pääsynhallinta toteutetaan Windows-palve-

linympäristössä. Lisäksi opin salasana-auditoinnin toteuttamisen Windows-aktiivihakemistoympäristössä ja useita salasanojen murtamiseen käytettäviä menetelmiä. Työssä ongelmia tuotti selkeästi kirjoitetun dokumentaation löytäminen siitä, miten salasanoja säilytetään aktiivihakemistossa sekä rainbow tablejen vähäinen saatavuus ilmaiseksi.

Järjestelmien siirtyessä virtuaalisiksi ja pilvipalveluihin, kuten aktiivihakemiston siirtäminen Microsoftin Azure-pilvialustalle (Azure AD), salasanojen auditointi toivottavasti helpottuu. Monet pilvialustat tarjoavat helposti hallittavissa olevan käyttöliittymän. Niiden avulla voi ottaa käyttöön esimerkiksi menetelmän, jossa salasanan luomisvaiheessa verrataan salasanaa sanalistaan, mikä estää heikkojen salasanojen käytön.

LÄHTEET

Apostol, A. (2013). A Novice's Guide to Password Cracking. Hakin9 04/2013(10), 45-52.

Arya, K. (2016). *Windows Group Policy Troubleshooting*. 1. painos. New York: Apress.

Boller, M. (2017). Cracking Active Directory Passwords. Haettu 20.02.2018 osoitteesta https://www.sans.org/reading-room/whitepapers/testing/cracking-active-directory-passwords-how-cook-ad-crack-37940

Bosworth, S. Kabay, M. E. Whyne, E. (2014). *Computer Security Handbook*. 6. painos. New Jersey: Wiley.

Clines, S. Loughry, M. (2008). *Active Directory for Dummies*. 2. painos. New Jersey: Wiley.

Dionach (2018). NtdsAudit v2.0.5. Haettu 16.02.2018 osoitteesta https://github.com/Dionach/NtdsAudit/releases

EC-Council (2010). *Ethical Hacking & Countermeasures – Attack Phases.* 1. painos. New York: EC-Council Press.

Gibson, D. (2015). *SSCP Systems Security Certified Practitioner All-in-One Exam Guide*. 2. painos. New York: McGraw-Hill Education.

Gordon, A. (2015). *Official (ISC)² Guide to the CISSP CBK*. 4. painos. Florida: CRC Press.

Greenberg, A. (2016). Hacker Lexicon: What is Password Hashing? Haettu 11.02.2018 osoitteesta https://www.wired.com/2016/06/hacker-lexicon-password-hashing/

IntiGrow (2018). Information Security Audits. Haettu 19.01.2018 osoitteesta http://intigrow.com/information-security-audits.html

Jungles, P. Simos, M. Grimes, R. Margosis, A. & Robinson, L. (2012). Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques. Haettu 04.02.2018 osoitteesta https://www.microsoft.com/en-us/download/details.aspx?id=36036

LearnCryptography (n.d.). Rainbow Tables. Haettu 17.02.2018 osoitteesta https://learncryptography.com/hash-functions/rainbow-tables

Lujan, V. (2017). What is Active Directory Anyway. Haettu 21.01.2018 osoitteesta https://jumpcloud.com/blog/what-is-active-directory-anyway/

MacGregor, T. (2000-2002). Password Auditing and Password Filtering to Improve Network Security. Haettu 21.01.2018 osoitteesta https://www.giac.org/paper/gsec/723/password-auditing-password-filtering-improve-network-security/100811

Maida, K. (2016). What the New NIST Guidelines Mean for Authentication. Haettu 28.01.2018 osoitteesta https://auth0.com/blog/what-the-new-nist-guidelines-mean-for-authentication/

Microsoft (2014). Active Directory Structure and Storage Technologies. Haettu 01.03.2018 osoitteesta https://technet.microsoft.com/library/cc759186(v=ws.10).aspx

Microsoft (2016). Ntdsutil. Haettu 20.01.2018 osoitteesta https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc753343(v=ws.11)

Microsoft (n.d.). Getting Started with Windows PowerShell. Haettu 27.02.2018 osoitteesta https://docs.microsoft.com/en-us/powershell/scripting/getting-started/getting-started-with-windows-powershell?view=powershell-6

NIST (2017). Digital Identity Guidelines Authentication and Lifecycle Management. Haettu 26.01.2018 osoitteesta http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

Parikh, J. (2013). An Introduction to Password Cracking. Hakin9 04/2013(10), 19-32.

Skullsecurity (n.d.). Passwords. Haettu 18.02.2018 osoitteesta https://wiki.skullsecurity.org/Passwords

Thomas, O. (2016). Windows Server 2016 Inside Out. Lontoo: Pearson Education.

Viestintävirasto (n.d.). Salasanat haltuun. Haettu 05.03.2018 osoitteesta https://www.viestintavirasto.fi/attachments/tietoturva/Salasanat_haltuun.pdf

Weir, M. Aggarwal, S. Collins, M. Stern, H. (2010). Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. Haettu 24.01.2018 osoitteesta http://www.cs.umd.edu/~jkatz/security/downloads/passwords_revealed-weir.pdf