MAANPUOLUSTUSKORKEAKOULU

VERKKOTIEDUSTELUN KOHTEET JA TEKNISET TIEDUSTELUMENETELMÄT

Kandidaatintutkielma

Kadetti
Jarno Tuominen

kadettikurssi 98
tiedusteluopintosuunta

maaliskuu 2014

MAANPUOLUSTUSKORKEAKOULU

Kurssi kadettikurssi 98	Linja tiedusteluopintosuunta	
Tekijä Kadetti Jarno Tuominen		
Tutkielman nimi **Verkkotiedustelun kohteet ja tekniset tutkimusmenetelmät**		
Oppiaine, johon työ liittyy Sotatekniikka	Säilytyspaikka MPKK (Kurssikirjasto)	
Aika maaliskuu 2014	Tekstisivuja 24	Liitesivuja 0

TIIVISTELMÄ

Kyberuhat ovat nousseet viime vuosina näkyvään rooliin ihmisten elämässä. Kyberhyökkäyksiä on myös mahdollista käyttää sotatoimien yhteydessä tai sotatoimien korvikkeena, kuten Stuxnet-haittaohjelmaa käytettiin. Verkkotiedustelu on olennainen osa kyberhyökkäyksiä, ja mahdollinen tuleva hyökkäys voi paljastua tiedustelun aikana.

Tutkimuksen päätutkimuskysymyksenä on ”Mitä on verkkotiedustelu?”. Kysymyksen alakysymyksinä on ”Mitä tietoverkoista tiedustellaan?” ja ”Miten tietoverkkoja tiedustellaan?”. Tutkimusmenetelmänä on kirjallisuuskatsaus. Pääasialliset lähteet ovat kyberturvallisuuteen ja verkkotunkeutumiseen liittyvä kirjallisuus sekä muut aiheeseen liittyvät eri virastojen julkaisut.

Verkkotiedustelun kohteena voi olla mikä tahansa organisaatio, jolla on jotain hyökkääjän haluamaa tietoa tai hyökkääjä saavuttaa jonkin päämäärän kohteeseen hyökkäämällä. Kohteeseen voidaan suorittaa kohdistettu hyökkäys tietojen kaappaamiseksi tai kohde voi olla osa kriittistä infrastruktuuria, jolloin hyökkäyksellä vaikutetaan fyysiseen maailmaan. Varsinainen tiedustelu tapahtuu kolmessa vaiheessa: julkisten lähteiden tutkiminen, verkon skannaaminen ja haavoittuvuuksien selvittäminen. Tiedustelu alkaa laajasti keräämällä mahdollisimman paljon tietoa kohteesta ja päättyy yhteen tai useampaan pisteeseen, joista murto kohteeseen on mahdollista.

Verkkotiedustelu on olennainen osa nykyaikaista kybersodankäyntiä. Verkkotiedustelu on yksinkertaistettuna hyökättävän kohteen etsimistä. Etsiminen voi kohdistua uuden kohteen löytämiseen tai se voi kohdistua tiedon hankkimiseen löydetystä kohteesta. Päätavoitteena kuitenkin on järjestelmään murtautumisen mahdollistaminen. Hyvin suoritetun tiedustelun jälkeen hyökkääjän on mahdollista suorittaa oma tehtävänsä kohteessa, eikä kohde havaitse hyökkäystä ennen kuin on liian myöhäistä.

AVAINSANAT
kyberturvallisuus, verkkohyökkäykset, automaatiojärjestelmät, verkkotiedustelu, kohdistettu hyökkäys, Advanced Persistent Threat, APT, teollisuusautomaatio, kriittinen infrastruktuuri, SCADA, porttiskannaus

SISÄLLYSLUETTELO

VERKKOTIEDUSTELUN KOHTEET JA TEKNISET TIEDUSTELUMENETELMÄT

1 JOHDANTO

Erilaiset kyberuhat ovat nousseet viime vuosina näkyviin myös tavallisen kansalaisen elämässä. Erityyppisiä palvelunestohyökkäyksiä tapahtuu Internetissä jatkuvasti. Palvelunestohyökkäykset ovat kuitenkin vain pieni, mutta hyvin näkyvä, osa kaikista Internetin kautta tulevista kyberuhista. Stuxnet-verkkomato hyökkäsi vuonna 2010 Iranin ydinlaitoksiin ja aiheutti fyysistä vahinkoa uraanin rikastamiseen käytetyille laitteille syöttämällä niille vääriä ohjaustietoja. Internetin kautta ja muita tietoverkkoja hyödyntämällä voidaan vaikuttaa tavallisen kansalaisen palveluihin tai mahdollisesti jopa sotilaskohteisiin.

Palvelunestohyökkäys on helppo toteuttaa pienillä valmisteluilla, mutta Stuxnetin kaltaisen laajemman hyökkäyksen tekeminen vaatii hyvää tuntemusta kohteena olevasta järjestelmästä. Aivan kuten tavanomaisessakin sodankäynnissä, täytyy hyökkäyksen kohde tiedustella ennen varsinaista iskua. Verkkotiedustelu on osa tätä hyökättävän kohteen tiedustelua. Verkkotiedustelun avulla voidaan tietoverkoista löytää hyökkääjää kiinnostavia kohteita, joihin pystytään varsinaisessa hyökkäyksessä vaikuttamaan. Palvelunestohyökkäyksessä tiedusteluksi voi riittää esimerkiksi lamautettavan www-sivun osoitteen selvittäminen, kun taas Stuxnet vaati syvällisempää tuntemusta kohteen verkosta.

Tietämällä miten verkkoja tiedustellaan, voidaan omat järjestelmät suojata tiedustelua vastaan, sekä testata omien suojausten toimivuus yrittämällä itse käyttää tiedustelussa käytettäviä menetelmiä omia järjestelmiä vastaan. Vaihtoehtoisesti voidaan myös tiedustella verkkoon päässyttä tiedustelijaa tai hyökkääjää ja selvittää tiedustelijan aikeet mahdollisessa hyökkäyksessä.

Tutkimuksessa käsitellään verkkotiedustelua osana Stuart McCluren, Joel Scambrayn ja George Kurtzin kuvaamaa hakkeroinnin prosessia. Prosessi alkaa kohteen tiedustelulla, joka toteutetaan kolmessa vaiheessa. Ensimmäisessä vaiheessa selvitetään mahdollisimman paljon tietoa kohteesta keräämällä tietoa julkisista lähteistä. Toisessa vaiheessa selvitetään mahdolliset hyökkäysreitit kohteeseen. Tiedustelun kolmas vaihe keskittyy haavoittuvuuksien, käyttäjätilien ja verkkoresurssien selvittämiseen. Tiedustelu voi varsinkin kolmannessa vaiheessa vaikuttaa hyökkäykseltä kohteessa. [1]

Tiedustelun jälkeen hyökkääjä murtautuu järjestelmään hyödyntäen tiedustelussa saatuja tietoja. Sisäänpääsyn jälkeen hyökkääjä pyrkii laajentamaan omia käyttöoikeuksiaan järjestelmästä, jotta pystyisi jatkamaan tehtäväänsä. Seuraavaksi hyökkääjä suorittaa haluamansa tehtävän kohteessa ja esimerkiksi voi siirtää tiedostoja pois kohdeverkosta. Hyökkääjä pyrkii tehtävän suorittamisen jälkeen sekä mahdollisesti sen vaiheissa peittämään jälkensä, jottei hyökkäys keskeydy tai hyökkääjän olemassa olo paljastu. Kohdejärjestelmään voidaan myös tehdä takaovia, joiden kautta hyökkääjä pääsee takaisin järjestelmään niin halutessaan. Hyökkäyksen epäonnistuessa, voidaan kohde pyrkiä lamauttamaan palvelunestohyökkäyksellä. [1]

1.1 Tutkimuskysymykset

Tutkimuksen on tarkoitus vastata kysymykseen "Mitä on verkkotiedustelu?". Pääkysymyksen apuna on kaksi alakysymystä, joihin vastaamalla pyritään vastaamaan pääkysymykseen.

Ensimmäinen alakysymys on "Mitä tietoverkoista tiedustellaan?". Tämän kysymyksen avulla selvitetään ensiksi kohdistetun hyökkäyksen muodostamaa uhkaa eri organisaatioille. Toiseksi pyritään selvittämään verkosta löytyviä kriittisen infrastruktuurin osia, jotka saattavat kiinnostaa erityyppisiä hyökkääjiä.

Toinen alakysymys on "Miten tietoverkkoja tiedustellaan?". Tämä kysymys käsittelee menetelmiä ja työkaluja, joita käytetään verkkojen tiedustelussa. Tällä kysymyksellä käsitellään erilaisten verkon skannaamiseen tarkoitettujen työkalujen toimintaa.

1.2 Tutkimuksen rajaus

Aihetta käsitellään teknisestä näkökulmasta. Tutkimus rajataan käsittelemään verkkotiedusteluun käytettäviä teknisiä keinoja, keskittyen verkon rakenteen ja palveluiden selvittämiseen käytettäviin menetelmiin. Näin työstä rajautuu pois esimerkiksi sosiaalinen manipulointi (social engineering), joka on yksi tiedustelussa ja kohteeseen murtautumisessa käytettävä keino, mutta ei perustu teknisiin keinoihin. Myös varsinainen verkkoon murtautuminen on rajattu työstä pois, vaikka tiedustelun viimeinen vaihe on jo lähellä verkkoon hyökkäämistä.

Tutkimuksessa ei myöskään käsitellä tietoverkoissa teknisin keinoin tapahtuvaa vakoilua tai muuta tiedonurkintaa, jota voidaan myös käyttää hyökättävän kohteen tiedustelussa, sillä ne ovat osa laajempaa kohdetta koskevaa tiedustelua, eivätkä välttämättä liity kohteen verkon rakenteen ja palveluiden selvittämiseen.

1.3 Tutkimusmenetelmä, aikaisemmat tutkimukset ja lähdemateriaalin esittely

Tutkimusmenetelmänä tässä tutkimuksessa käytetään kirjallisuustutkimusta. Käytettävät lähteet ovat aikaisemmat aihetta käsittelevät ja sivuat tutkimukset, aiheesta kertova kirjallisuus, erilaiset muut julkaisut ja raportit sekä erilaiset Internet-lähteet.

Aihetta käsittelee Mika Pullisen Laurea-ammattikorkeakoulussa tehty opinnäytetyö ”Kriittisten tietojärjestelmien suojaaminen kyberuhilta”, joka käsittelee aihetta hyvin laajasti järjestelmiin hyökkäämisen kannalta. Samalla työssä käsitellään myös jonkin verran verkkotiedustelua ja verkkotiedustelun suojautumiskeinoja.

Tietojärjestelmien suojaamista tunkeutumisen havaitsemis- ja estojärjestelmillä käsitellään kahdessa opinnäytetyössä. Ensimmäinen on Jani Ekmanin Metropoliaan tehty opinnäytetyö, jonka aiheena on ”Tunkeutumisenesto ja havainnointi käytönvalvontajärjestelmissä”. Toinen on Mika Luukkasen Lahden ammattikorkeakoulussa tehty opinnäytetyö ”Tunkeutumisen havaitsemisjärjestelmän käyttöönotto”. Näistä ensimmäinen käsittelee myös käytönvalvontajärjestelmiä, jotka voivat olla osana esimerkiksi kriittistä infrastruktuuria.

Penetraatiotestaus liittyy myös verkkotiedusteluun ja verkon suojaamiseen. Tätä aihetta käsittelee Jarkko Puhakan Jyväskylän Ammattikorkeakoulussa tehty opinnäytetyö ”Penetraatiotestaus osana tietoturvan toteutusta”.

Tuoreinta tutkimustietoa edustaa maaliskuussa 2013 Aalto-yliopistossa tehty selvitys ”Suomen automaatioverkkojen haavoittuvuus”, jossa etsittiin Internetiin näkyviä automaatiolaitteita Shodan-hakukoneella.

Lähdemateriaalina tässä tutkimuksessa on käytetty edellä mainittujen tutkimusten lisäksi aihetta käsittelevää kirjallisuutta. Keskeisimpänä lähteenä on kirja ”Cyber warfare: techniques, tactics and tools for security practitioners”. Kirja käsittelee laajasti kybersodankäyntiä muun muassa kybermaailman toimijoista, työkaluista ja jopa toiminnan eettisyydestä. Toinen laajasti aihetta käsittelevä teos on Lech J. Janczewskin ja Andrew M. Colarikin ”Cyber warfare and cyber terrorism”. Varsinaisia tiedusteluun käytettäviä tekniikoita käsitellään kirjassa ”Hacking Exposed 7: Network Security Secrets & Solutions”, joka käsittelee myös verkkohyökkäyksien toteuttamista käytännössä.

Lähteinä on käytetty myös Maanpuolustuskorkeakoulun omia julkaisuja ”The fog of cyber defence” ja ”Cyber Warfare”. Muina lähteinä ovat muun muassa erilaisten kotimaisten virastojen kuten Valtiovarainministeriön sekä CERT-FI:n julkaisut sekä Internet-lähteitä, kuten yleisimmän porttiskanneri Nmapin käyttöohje. Tutkimuksessa on käytetty myös Wikipedia-artikkeleita lähteinä tietoteknisiin peruskäsitteisiin, jotka eivät ole muuttuneet juurikaan viime vuosina.

1.4 Määritelmät

haavoittuvuus	Ohjelmistossa oleva virhe, joka mahdollistaa esimerkiksi ohjelmiston väärinkäytön
haittaohjelma	Ohjelma, jonka tarkoituksena on aiheuttaa haittaa tietokoneessa tai tietojärjestelmässä
IP-osoite	Internetiin kytketyn laitteen verkko-osoite. Koostuu neljästä pisteellä erotetusta luvusta väliltä 0-255. Esimerkiksi 80.248.161.40
palomuuri	Laite tai sovellus joka valvoo verkkoliikennettä ja sallii vain halutun liikenteen lävitseen
palvelunestohyökkäys	Hyökkäys, jossa häiritään tai estetään palvelun toimintaa
portti	TCP/IP-yhteyksissä tietokoneessa olevan palvelun kanssa kommunikointiin käytettävä osoitteen osa
porttiskannaus	Menetelmä, jossa verkosta etsitään tietokoneita ja niissä olevien avoimien porttien perusteella tietokoneen tarjoamia palveluja.
SCADA	Supervisory Control And Data Acquisition, esimerkiksi teollisuusautomaatiossa käytettävä käytönvalvontajärjestelmä
TCP/IP	Protokollaperhe, joka vastaa tiedon liikkumisesta verkoissa.
tietojärjestelmä	tietoverkosta, ihmisistä ja ohjelmistoista koostuva kokonaisuus joka helpottaa jonkin toiminnan tekemistä
tietoturva-aukko	Heikkous tietojärjestelmässä, joka mahdollistaan järjestelmään tunkeutumisen
tietoverkko	tietokoneista ja niitä yhdistävistä laitteista muodostuva verkko
verkkopalvelu	tietoverkon sen käyttäjille tarjoama palvelu, esimerkiksi tiedostojen tallennus verkkoon tai laitteen etäkäyttö

2 TIEDUSTELTAVAT KOHTEET

Tässä luvussa perehdytään verkkohyökkäyksille alttiisiin kohteisiin hyökkäystä edeltävän tiedustelun näkökulmasta. Mahdollisiksi kohteiksi valikoituivat kohdistetulle hyökkäykselle alttiit kohteet ja erilaiset automaatiojärjestelmät mukaan lukien kriittinen infrastruktuuri. Kohdistettua hyökkäystä voidaan käyttää jotakin yksittäistä yritystä vastaan tai jotakin valtion virastoa tai jopa puolustusvoimia vastaan. Kriittistä infrastruktuuria vastaan hyökkääminen mahdollistaa yhteiskunnalle kriittisten toimintojen lamauttamisen.

Erilaiset verkkohyökkäykset alkavat tiedustelulla. Tiedustelun avulla pyritään selvittämään kohteena olevasta organisaatiosta ja järjestelmästä mahdollisimman paljon. Tuntemus kohteen verkkoinfrastruktuurista, käytettävistä laitteista ja ohjelmistoista sekä kohteessa työskentelevistä ihmisistä on pohjana muun hyökkäyksen suunnittelulle. [2, s. 120]

Tiedustelu voidaan suorittaa kahdessa osassa. Ensin etsitään yleisesti kaikki mahdollinen saatavilla oleva tieto kohteesta ja tämän jälkeen voidaan keskittyä tarkemmin mahdollisen murron aikaan saavan aukon tiedusteluun. Jälkimmäisessä vaiheessa toteutettu tiedustelu tapahtuu suoraan liittyen kohteeseen murtautumiseen. Tällöin tiedustelun ei enää tarvitse olla niin huomaamatonta kuin yleisessä kohteen tiedustelussa. [3, s. 171] Tiedustelu voi tapahtua myös hyvin laajassa mittakaavassa, jossa etsitään useista järjestelmistä tärkeitä kohteita ja mahdollisia tulevaisuudessa sotatoimien yhteydessä käytettäviä aukkoja tietojärjestelmiin. Yhteen järjestelmään tehty suuri hyökkäys voi olla vaikea toteuttaa, mutta monta hyökkäystä pienempiä järjestelmiä vastaan voi olla helpompaa tehdä. [4, s. 36]

2.1 Kohdistetut hyökkäykset

Mikä tahansa organisaatio, kuten yksityiset yritykset tai valtion virastot voivat joutua kohdistetun hyökkäyksen uhriksi. Kohdistetusta hyökkäyksestä voidaan käyttää myös englanninkielistä termiä Advanced Persistent Threat (APT) [5]. Kohdistetussa hyökkäyksessä ulkopuolinen taho pyrkii varastamaan jotakin tietoa kohteelta tai haitata kohteen toimintaa [6, s. 9]. Esimerkki kohdistetusta hyökkäyksestä on vuoden 2013 syksynä julki tullut Ulkoministeriön verkkoon murtautuminen.

Kohdistetun hyökkäyksen kohde on harkittu. Kohde valitaan siitä saatavan hyödyn perusteella. Kohteella tiedetään olevan jotakin sellaista tietoa tai muuta hyökkääjää kiinnostavaa, mikä tekee hyökkäyksen kohdetta vastaan kannattavaksi. Tästä syystä hyökkäämiseen nähdään myös paljon vaivaa. Hyökkääjä ei luovuta heti vaikka hyökkäys pysähtyisi ensimmäisen esteeseen, vaan hyökkääjä pyrkii löytämään muun tavan päästä käsiksi kohteeseen. [6, s. 15]

Hyökkääjän tavoitteet määrittävät myös hyökkäyksen keston. Yksittäinen tietokaappaus kohteesta voidaan toteuttaa melko nopeasti, jonka jälkeen hyökkääjä voi poistua kohteen verkosta ja peittää omat jälkensä. Jos taas hyökkääjällä on tavoitteena pidempi aikainen kohteen vakoilu tai haitanteko kohteelle, voi hyökkääjä olla kohteen verkossa jopa vuosia. Hyökkäyksen pidentyessä myös hyökkääjän riski paljastua kasvaa.[5]

Kohdistetun hyökkäyksen toteuttajana voi olla esimerkiksi valtio, verkkorikolliset, aktivistit tai jopa kilpaileva yritys [7, s. 80–81]. Valtiollisilla toimijoilla tai valtioiden tukemilla toimijoilla on yleensä paremmat resurssit toimintaan kuin esimerkiksi erilaisilla aktivistiryhmillä, jotka ovat motivoituneita oman aatteensa levittämisestä. Verkkorikollisilla on usein taloudelliset tavoitteet. [3, s. 30] Verkkorikolliset voivat kohdistaa hyökkäyksensä esimerkiksi kauppaketjun järjestelmiin, joista ne pyrkivät varastamaan asiakkaiden luottokorttitietoja.

Hyökkäys voidaan toteuttaa esimerkiksi haittaohjelmilla. Haittaohjelmat voivat hyödyntää tietoturva-aukkoja kohteen käytössä olevissa järjestelmissä. Esimerkiksi haittaohjelma voi hyödyntää haavoittuvuutta kohteen käyttämässä toimisto-ohjelmistossa. Hyökkääjä laatii hyvin asialliselta vaikuttavan asiakirjan ja lähettää sen sähköpostin liitteenä oikealle henkilölle kohdeorganisaatiossa. Henkilön avatessa täysin tavalliselta vaikuttavan liitetiedoston, käynnistyy haittaohjelma ja hyökkääjä pääsee kohteen tietojärjestelmään. Saastunutta konetta voidaan käyttää hyökkäyksen sillanpääasemana, jonka kautta hyökkääjä pääsee jatkamaan toimintaansa verkossa. [5]

Kohdistetun hyökkäyksen tekeminen vaatii luonnollisesti huolellista tiedustelua ennen hyökkäystä. Käytännössä kaikki mahdollinen tieto kohteesta auttaa. Tekniset tiedot, kuten kohteen käyttämät tietojärjestelmät ja erilaiset ohjelmistot, kuten toimisto-ohjelmat, voivat mahdollistaa jonkin kohteen käyttämän järjestelmän haavoittuvuuden hyödyntämisen hyökkäyksessä. Tiedustelun perusteella voidaan esimerkiksi hyökkäyksessä käytettävä sähköpostiviesti tehdä mahdollisimman todenmukaiseksi. [5]

Tiedustelulla pyritään selvittämään keinot joilla kohteen järjestelmiin päästään käsiksi. Tämä tarkoittaa mahdollisia haavoittuvaisia ohjelmistoja, joiden tietoturva-aukkoja voidaan hyödyntää varsinaisessa hyökkäyksessä. Yleisiä hyökkäykseen käytettäviä ohjelmistoja ovat esimerkiksi kohteen käyttämät toimisto-ohjelmat, eli tekstinkäsittely-, taulukkolaskenta- ja esitysovellukset. Hyökkääjä voi esimerkiksi laatia asiakirjan, joka sisältää tekstinkäsittelyohjelmassa olevaa haavoittuvuutta hyväksikäyttävän haittaohjelman. Haittaohjelmaa voidaan levittää myös muilla keinoilla. Kohteen työntekijä voidaan ohjata haittaohjelman sisältämälle www-sivulle, jolloin haittaohjelma hyödyntää verkkoselaimessa olevaa haavoittuvuutta. Haittaohjelma voi levitä myös muistitikkujen välityksellä, jolloin voi riittää pelkästään muistitikun liittäminen tietokoneeseen jolloin haittaohjelma käynnistyy. [5] Tämä hyödyntää haavoittuvuutta itse tietokoneen käyttöjärjestelmässä. Muistitikuilla voidaan haittaohjelmaa levittää myös sellaisiin järjestelmiin, jotka eivät ole yhteydessä Internetiin, kuten esimerkiksi korkeamman turvallisuusluokan verkkoihin. [7, s. 82]

Kaikki tieto kohteen verkon rakenteesta kiinnostaa hyökkääjää. Verkon ulkopuolelta hyökkääjä pystyy tiedustelemaan ulkoverkkoon yhteydessä olevia laitteita. Näitä ovat esimerkiksi www- ja sähköpostipalvelimet. Haavoittuvuus tällaisessa palvelussa mahdollistaa kohteeseen murtautumisen suoraan ulkoverkosta. Kohdetta kiinnostava tieto ei välttämättä ole suoraan siinä pisteessä, josta hyökkääjä on päässyt kohteen järjestelmään sisään, vaan se voi olla muualla. Kohteelta kaapattu tieto täytyy myös siirtää kohteen verkosta pois. Tuntemalla kohteen verkko, voi hyökkääjä etsiä haluamansa tiedon kohteelta tai muodostaa turvallisen ja huomaamattoman reitin ulos, jota pitkin tietoa voidaan siirtää kohdeverkosta. Verkon tarkempi tutkiminen voi kuitenkin alkaa vastaa haittaohjelman aktivoitumisen jälkeen. Saastuneen tietokoneen kautta hyökkääjä voi jatkaa verkon tiedustelua, kuten muiden laitteiden ja uusien haavoittuvuuksien etsimistä kohdeverkosta.

Myös aivan ”tavallinen” tiedustelutieto kohteesta kiinnostaa hyökkääjää. Esimerkiksi tiedot kohteen työntekijöistä, asiakkaista ja käynnissä olevista hankkeista auttaa hyökkääjä kohdentamaan hyökkäystä. Esimerkiksi haittaohjelmalla varustettu asiakirja voidaan laatia siten että se vaikuttaa liittyvän johonkin käynnissä olevaan hankkeeseen. Kohteen työntekijä tuskin avaa täysin roskapostilta vaikuttavaa sähköpostiviestiä, mutta jos viesti vaikuttaa täysin tavalliselta jokapäiväiseen työhön liittyvältä, työntekijä todennäköisesti avaa viestin ja siihen liitetyn asiakirjan.

2.2 Automaatiojärjestelmät ja kriittinen infrastruktuuri

Monia fyysisen maailman palveluja ohjataan erilaisten tietoteknisten järjestelmien avulla. Nämä tietotekniset järjestelmät toimivat fyysisten laitteiden avulla. Tämä mahdollistaa hyökkäämisen näitä kohteita vastaan tavallisen sodankäynnin keinoin itse fyysistä laitetta vastaan tai kyberhyökkäyksellä laitetta hallitsevaa ohjelmaa vastaan. Muutokset järjestelmien ohjelmistoissa tai laitteistoissa vaikuttavat toisiinsa ja mahdollisesti muihin järjestelmiin. Esimerkiksi sähkön ja verkkoyhteyden katkeaminen tällaisesta järjestelmästä voi tehdä siitä sillä hetkellä täysin hyödyttömän. [3, s. 119–120]

Erilaisia automaatiojärjestelmiä on käytössä monissa paikoissa. Erilaisten tuotantolaitosten prosesseja ohjataan tietokoneiden avulla. Kiinteistöissä voidaan ilmanvaihtoa, lämmitystä ja jopa ovien lukituksia ohjata jollakin tietoteknisellä järjestelmällä. Myös kriittisen infrastruktuurin palveluita ohjataan erilaisilla automaatiojärjestelmillä. Kriittinen infrastruktuuri kattaa palvelut, joita ilman ihmisten jokapäiväinen elämä vaikeutuisi paljon. Esimerkkeinä kriittisen infrastruktuurin palveluista ovat esimerkiksi sähköntuotanto ja -jakelu, vedenjakelu, pankkipalvelut, viestintäverkot ja logistiikka [4, s. 36]. Tällaiset palvelut toteuttavat tai tukevat toimintoja jotka puuttuessaan voisivat lamauttaa yhteiskuntaa tai vaikuttaa ihmisten turvallisuuteen. Esimerkiksi nykyään hyvin moni palvelu toimii sähkön avulla ja katkokset sähkön saannissa voivat estää monen palvelun toimivuuden.

Näitä automaatiojärjestelmiä kutsutaan myös termillä SCADA (Supervisory Control and Data Acquisition). [3, s. 21] SCADA-järjestelmiä käytetään erilaisten toimintojen ohjaamiseen ja valvontaan. Teollisuuden käytössä järjestelmät ovat tuotantolaitoksissa, kuten energiantuotannossa, öljynjalostuksessa, kaivostoiminnassa tai muissa tehdasoloissa tapahtuvissa toiminnoissa. Infrastruktuurin liittyviä toimintoja, kuten vedenjakelua, sähkönjakelua ja erilaisia viestintäverkkoja ohjataan myös SCADA-järjestelmillä. Rakennuksissa näillä järjestelmillä ohjataan esimerkiksi lämmitystä ja ilmastointia. Ilman tällaisia järjestelmiä pitämässä yhteiskuntaa pystyssä, olisimme nopeasti ilman lämmitystä, ruokaa, viestiyhteyksiä ja muita mukavuuksia. Vaikka kriittiset järjestelmät voivat olla moneen kertaan kahdennettuja, perustuvat ne kuitenkin tietokoneisiin ja ovat siten haavoittuvaisia. [3, s. 123–124]

Tiedusteltaessa automaatiojärjestelmiä täytyy ensin löytää haluttu kohde. Terroristeille ja aktivisteille voi riittää mikä tahansa kohde jolla voi vaikuttaa fyysiseen maailmaan kun taas valtiollisia toimijoita voi kiinnostaa kohteet joilla saadaan oikeasti lamautettua muitakin palveluita, esimerkiksi sähköntuotanto tai -jakelu. Automaatiojärjestelmiä voi löytää suoraan Internetistä, sillä niissä olevan tiedon pitää olla saatavilla laitetoimittajille ja järjestelmän käyttäjille vuorokauden ympäri [8, s. 4]. Toisaalta jokin järjestelmä on voitu kytkeä Internetiin vahingossa. Vahingossa Internetissä olevat järjestelmät voivat lisäksi päästää käyttäjän suoraan käyttämään järjestelmää ilman käyttäjän tunnistusta, sillä järjestelmän ei ole tarkoitus edes näkyä Internetissä.

Suoraan Internetiin näkyviä järjestelmiä voidaan etsiä myöhemmin tutkielmassa esiteltävällä porttiskannauksella tuntemalla järjestelmän käyttämät portit. Yleinen harhaluulo tietoturvan suhteen on luottaminen security through obscurity -ajatteluun. Järjestelmiä ei välttämättä ole ollenkaan suunniteltu käytettäväksi Internetin yli. Järjestelmät ovat alun perin olleet käytössä suljetuissa verkoissa, jotka ovat jälkeenpäin yhdistetty julkiseen verkkoon. Ylläpitäjät ovat ajatelleet, ettei kyseisiä järjestelmiä ole mahdollista löytää Internetistä. Järjestelmiä on tehty ajatellen, ettei kukaan haluaisi tai edes pystyisi murtautumaan järjestelmään, koska se on suunniteltu uniikiksi järjestelmäksi vain yhteen käyttöön. [3, s. 22] Koska järjestelmä on rakennettu yhtä tarkoitusta varten, eivätkä ulkopuoliset henkilöt tunne järjestelmän liityntöjä, ohjelmistoja, käyttöjärjestelmiä tai protokollia, luullaan järjestelmään murtautumisen olevan vaikeaa. Järjestelmätoimittajat kuitenkin laittavat Internetiin käyttäjän ja samalla kaikkien muidenkin nähtäville ohjekirjoja, joten henkilö joka haluaa yksityiskohtaista tietoa jostakin järjestelmästä saattaa löytää sen Internetin kautta. [3, s. 124] Tällaiset mahdolliset tietoturvapuutteet tekevät monista SCADA-järjestelmistä kohteita verkkohyökkäyksille ja samalla myös tiedusteltavia kohteita.

Laitteen löytämisen jälkeen hyökkääjän täytyy päästä käyttämään järjestelmää. Jotkin järjestelmät voivat päästää kenen tahansa käyttämään järjestelmää ilman minkäänlaista käyttäjäntunnistusta. Tämä johtunee siitä että järjestelmä on tarkoitettu käytettäväksi suljetussa verkossa monen eri käyttäjän toimesta. Toisaalta järjestelmässä voi olla jokin haavoittuvuus jota ylläpito ei ole korjannut tai se ei ole tietoinen siitä. Järjestelmä voivat olla vanhoja, eikä ylläpidolla välttämättä ole testiympäristöä järjestelmämuutosten testaamiseen [3, s. 22]. Tällöin järjestelmän päivityksiä ei voida testata etukäteen ja tuotantojärjestelmän päivittäminen suoraan voi olla riskialtista. Ylläpitäjät eivät pidä järjestelmän päivittämistä tärkeänä, sillä luulevat sen olevan ulkopuolisten tavoittamattomissa. Esimerkiksi Stuxnet osoitti että mahdollisen iskun tekijöiltä löytyy tarvittaessa osaaminen jopa uraanin rikastuslaitoksen toiminnanohjausjärjestelmistä ja jopa osaaminen saada kyseisen järjestelmän laitteet rikkomaan itsensä [9, s. 221].

3 TIEDUSTELUMENETELMÄT

Tässä luvussa perehdytään tietoverkkojen tiedusteluun käytettäviin menetelmiin ja työkaluihin. Menetelmiä pyritään käsittelemään verkkotiedustelun prosessin mukaisesti. Verkkotiedustelu voidaan jakaa kolmeen osaan. Ensimmäisessä vaiheessa selvitetään pääasiassa täysin julkisia lähteitä käyttäen mahdollisimman paljon tiedusteltavasta kohteesta [1, s. 8]. Toisessa vaiheessa pyritään selvittämään mahdollisia hyökkäysreittejä kohteeseen käyttämällä erilaisia skannausmenetelmiä kuten porttiskannausta [1, s. 48]. Kolmannessa vaiheessa pyritään löytämään mahdollisia haavoittuvuuksia löydetyistä mahdollisista hyökkäysreiteistä [1, s. 84].

Menetelmien havaittavuus myös kasvaa tiedustelun edetessä. Julkisia lähteitä käytettäessä kohteesta voidaan saada tietoa lähettämättä yhtään pakettia kohdejärjestelmään, kun taas haavoittuvuuksien löytäminen voi vaatia monien pakettien lähettämistä, mikä jättää jälkiä kohdejärjestelmiin. Koska tiedustelun loppuvaiheissa järjestelmään jää jälkiä, ei tiedustelija halua jälkien johtavan häneen ja paljastavan tiedustelijaa tai tiedustelijan taustalla olevaa organisaatiota. Tiedustelussa voidaan käyttää erilaisia välityspalvelimia tai Tor-verkkoa, joiden avulla tiedustelija peittää oman alkuperänsä. [1]

Hyökkääjää kiinnostaa kaikki mahdollinen tieto kohteen verkko-osoitteista, kohteen käyttämistä IP-osoitteista, palvelimista ja verkon aktiivilaitteista sekä kaikki mahdollinen tieto liittyen kohteen verkon suojaamiseen. [1, s. 8-9]

3.1 Julkiset lähteet

Julkisista lähteistä tiedustelua kutsutaan myös termillä Open Source Intelligence (OSINT). Julkisia lähteitä käyttämällä kerätään kohteesta tietoa organisaation itsensä tai muiden organisaatioiden kohteesta julkaisemista tiedoista. Tällainen toiminta on passiivista sillä julkisten lähteiden tutkiminen ei jätä tavallisesta poikkeavia jälkiä kohteen järjestelmiin[3, s. 157]. Julkisia lähteitä ovat esimerkiksi erilaiset kohteen julkaisemat asiakirjat. Mahdollisesti julkiset tarjouskilpailut voivat paljastaa kohteen käyttämiä laitteita. Käynnissä olevat ja menneet hankkeet ja tiedot henkilöiden asemasta organisaatiossa mahdollistavat sosiaalisen manipuloinnin hyödyntämisessä tiedustelun tukena tai varsinaisessa hyökkäyksessä.

Kohdeorganisaation Internet-sivut voivat pitää sisällään esimerkiksi ohjeet organisaation VPN-palvelun (Virtual Private Network) tai jonkin muun organisaation palvelun käyttämiseen, mitkä voivat olla mahdollisia hyökkäysreittejä hyökkääjälle [1, s. 12]. Kohteen verkkosivut voivat myös viitata johonkin kohteen kanssa yhteistyötä tekevään organisaatioon [1, s. 13]. Kohteeseen voidaan hyökätä hyödyntäen yhteyttä löydettyyn toiseen organisaatioon esimerkiksi hyökkäämällä yhteistyöorganisaation kautta.

Vaikka sosiaalinen manipulointi on rajattu tämän tutkimuksen ulkopuolelle, niin julkisista lähteistä tapahtuvan tiedustelun avulla löydetään paljon sosiaalista manipulointia mahdollistavaa tietoa. Varsinkin ihmisiin liittyviä tietoja, kuten nimiä, puhelinnumeroita, osoitteita, organisaatiorakenteita voidaan käyttää sosiaalisessa manipuloinnissa sekä hyökkäyksen kohdistamiseen [2, s. 122]. Julkisista lähteistä voi löytää myös tietoa kohteen teknisistä järjestelmistä, kuten IP-osoitteita, tietoa verkon rakenteesta, ohjelmistoista ja laitteista [2, s. 122]. Esimerkiksi ilmoitus avoimesta työpaikasta voi pitää sisällään osaamisvaatimuksia tietyistä kohteen käytössä olevista järjestelmistä ja näin epäsuorasti vuotaa tietoa myös tiedustelijalle [1, s. 17].

Esimerkiksi kohdeorganisaation julkaisemat asiakirjat voivat paljastaa organisaation käyttämät toimisto-ohjelmat. Kohdetta vastaan voidaan tällöin hyökätä hyödyntäen toimisto-ohjelmassa olevaa tietoturva-aukkoa. Sama pätee myös sähköpostiviesteihin. Sähköpostipalvelimet ja -ohjelmat jättävät jälkensä sähköpostiviestien ohjaamiseen tarkoitettuihin tietoihin. Näiden tietojen perusteella voidaan päätellä kohdeorganisaation käyttämät sähköpostijärjestelmät ja mahdollisesti hyökätä kohteeseen hyödyntämällä tietoturvaturva-aukkoa organisaation sähköpostijärjestelmässä.

3.1.1 DNS ja WHOIS

Internetissä olevilla tietokoneilla ja laitteilla on jokin IP-osoite. IP-osoitteet muodostuvat neljästä pisteellä erotetusta numerosta. Numerot ovat käteviä tietokoneille, mutta ihmisen on vaikea muistaa pitkiä numerosarjoja. Tätä varten kehitettiin nimipalvelu, (Domain Name System, DNS). Nimipalvelu muuttaa ihmiselle helpomman tekstimuotoisen verkkotunnuksen esimerkiksi www.puolustusvoimat.fi tietokoneiden ymmärtämään numeromuotoon 80.248.161.40. Sama on mahdollista myös toisin päin, eli IP-osoitteesta saadaan tekstimuotoinen verkkotunnus, jos sellainen on olemassa.

Yleensä nimipalvelu palauttaa vain verkkotunnusta vastaavan IP-osoitteen tai toisin päin. nimipalvelimelta on kuitenkin mahdollista saada laajemmat tiedot kohde IP-osoitteesta käyttämällä zone transfer -operaatiota. Zone transfer -operaatio onnistuessaan palauttaa kaikki palvelimella olevat tiedot kyseisestä osoitteesta. [3, s. 89] Tällaisia tietoja ovat esimerkiksi kohteen sisäverkon laitteiden nimet ja osoitteet. Nämä kertovat hyökkääjälle paljon kohteen sisäverkosta ja helpottavat kohteen sisäverkon kohteita vastaan hyökkäämistä. [1, s. 37]

Nimipalvelimet eivät kuitenkaan yleensä toteuta satunnaisten tietokoneiden tekemiä zone transfer -pyyntöjä. Nimipalvelimelta voi kuitenkin kysyä muuta hyödyllistä informaatiota kuten kohdeorganisaation sähköpostipalvelimen osoitetta. [3, s. 89] Sähköpostipalvelimen kautta voidaan mahdollisesti päästä käsiksi kohde organisaation sisäverkkoon.

Whois-järjestelmä liittyy myös Internet-osoitteisiin. Whois-järjestelmän kautta saa tietoa verkkotunnusten rekisteröinnistä. Tiedot kertovat kuka on rekisteröinyt kyseisen nimen, kertoo rekisteröijän osoitteen ja organisaation käyttämät nimipalvelimet. [3, s. 87] Whois-järjestelmän avulla voi whois-palvelimesta riippuen pystyä selvittämään esimerkiksi kaikki tietyn nimipalvelimen hallinnoimat verkko-osoitteet [1, s. 31]. Nämä muut verkko-osoitteet voivat johtaa muihin kohdeorganisaation käyttämiin palveluihin. Whois-järjestelmän kautta saadaan myös ihmisiin liittyviä tietoja, jotka ovat käyttökelpoisia sosiaalisen manipuloinnin kanssa.

3.1.2 Hakukoneet

Hakukoneet kuten Google löytävät paljon edellä mainittua julkista tietoa pääasiassa koko Internetistä. Hakukoneissa on yleensä myös muita hakuoperaattoreita, joita hyödyntämällä voi haun kohdistaa tiettyyn verkkosivuun. Tätä kutsutaan myös termillä Google Hacking, Google hakkerointi [3, s. 86]. Esimerkiksi hakuparametrilla "intitle:" Google etsii sivujen otsikoista ja haulla intitle:"switch home page" voi löytää verkkokytkimien hallintasivuja. Hakuparametri "site:" etsii tietoa tietyltä sivustolta. Yhdistämällä hakuparametreja voidaan esimerkiksi etsiä kytkimien hallintasivuja tietystä osoitteesta ja näin mahdollisesti saada tietoa kohteen verkon aktiivilaitteista.[2, s. 125] Tiedon etsintään on myös useita kehittyneitä ohjelmistoja, jotka hyödyntävät useita eri hakukoneita ja tunnetuista hakuparametreista koottuja tietokantoja. Tällaiset ohjelmistot mahdollistavat tietojen keräämisen halutusta kohteesta automaattisesti. [1, s. 21–23]

Hakukoneeksi voidaan luokitella myös Shodan. Shodan on hakukone, jolla on tarkoitus etsiä muita tietokoneita tai laitteita. Sen tiedot perustuvat koko Internetin kattaviin porttiskannauksiin. Tästä syystä johtuen se ei anna täysin reaaliaikaista tietoa, vaan sen antamat tiedot voivat olla vanhentuneita. Jokin Shodanin löytämä laite on voinut poistua Internetistä tai sen IP-osoite on voinut muuttua Shodanin tekemän porttiskannauksen jälkeen. [10]

Shodanilla on esimerkiksi mahdollista etsiä tietyn valmistajan automaatiolaitteita. Shodanilla hakutuloksia on mahdollista rajata esimerkiksi valtion tai kaupungin perusteella, mikä mahdollistaa halutun kohteen tarkemman rajauksen. Tämä mahdollistaa esimerkiksi Suomessa olevien haavoittuvien automaatiolaitteiden etsimisen. Kyseistä tietoa voidaan käyttää oikeissa käsissä tietoturvan parantamiseen ja haavoittuvien laitteiden suojaamiseen, mutta sitä voidaan luonnollisesti käyttää myös järjestelmän hyväksikäyttöön. Shodanin avulla voidaan etsiä esimerkiksi haavoittuvaisia kohteita kriittisestä infrastruktuurista tulevia hyökkäyksiä tai terrorismia varten. Erilaiset aktivistit tai verkkorikolliset voivat sabotoida avointa automaatiojärjestelmää omien etujensa ajamiseen tai huomion herättämiseen. [10]

3.2 Verkon skannaaminen

Verkon skannaamiseen käytettävät työkalut ovat usein samoja, joita käytetään myös tietojärjestelmien turvallisuuden testaamiseen eli penetraatiotestaukseen. Penetraatiotestauksessa tietojärjestelmään yritetään murtautua käyttäen samantapaisia tai samoja työkaluja kuin pahantahtoinen hyökkääjä. [11, s. 55] Skannaamiseen käytettävät työkalut voivat olla ilmaisia tai jopa avoimen lähdekoodin ohjelmia, kuten Nmap. Verkon skannaaminen voidaan toteuttaa esimerkiksi haittaohjelman tai kyberaseen osaksi, jolloin haittaohjelma voi skannata esimerkiksi suljetun verkon laitteita ennalta määriteltyjen ohjeiden mukaisesti [7, s 85].

3.2.1 Ping-skannaus

Skannausmenetelmistä yksinkertaisin on ping-skannaus. Ping-skannaus hyödyntää verkon toiminnan tutkinnassa käytettyä monista käyttöjärjestelmistä löytyvää ping-ohjelmaa. Ping-ohjelmalla testataan onko jokin laite verkossa. Ping-ohjelmat lähettävät kohdelaitteelle ICMP echo request -paketin. Jos laite on olemassa, se lähettää vastauksena ICMP echo reply -paketin. [12]

Ping-skannauksella saadaan selville vastaako jokin laite ping-kyselyihin, Tästä voidaan päätellä onko kyseisessä osoitteessa olemassa päällä olevaa laitetta. Skannaamalla verkon kaikki IP-osoitteet, saadaan selville kaikki verkossa päällä olevat laitteet. Kaikki laitteet eivät kuitenkaan välttämättä vastaa ping-kyselyihin. ICMP-protokollan paketit voidaan suodattaa verkosta, sillä mahdollisen hyökkääjän käyttämänä niitä voidaan käyttää juuri verkon tiedusteluun. Tämä vaikeuttaa skannausta sillä vastauksen puuttuminen ei erittele suodatetaanko verkossa ICMP-paketteja vai puuttuuko kyseinen IP-osoite oikeasti verkosta. [12]

Yksittäinen ping-kysely käyttää liikenteeseen vain kaksi pakettia laitteiden välillä, joten se on melko huomaamaton. Vähäisestä pakettien lähetysmäärästä johtuen se on myös hyvin nopea, eniten aikaa kuluu puuttuvien vastausten odottamiseen. Koko verkon skannaaminen, eli kaikkien mahdollisten IP-osoitteiden läpikäyminen vaatii ping-kyselyn tekemisen jokaiseen IP-osoitteeseen. Tämä luo jo paljon enemmän verkkoliikennettä. [12]

3.2.2 Porttiskannaus

Seuraava menetelmä on porttiskannaus (port scan). Porttiskannauksella selvitetään laitteen avoimia portteja. Portti on TCP ja UDP -protokollien käyttämä ”palvelupiste”, joita tietokoneet käyttävät eri palveluiden erottamiseen TCP ja UDP protokollia käytettäessä. Saman IP-osoitteen tarjoamat eri palvelut erotetaan käyttämällä jokaisella palvelulla omaa porttia. Osa porteista on vakioituja, kuten HTTP:n käyttämä TCP portti numero 80.

Porttiskannauksessa lähetetään porttiin yksinkertainen paketti, johon porttia mahdollisesti kuunteleva palvelu vastaa tai ei vastaa. Vastauksesta päätellään onko kyseisessä portissa jokin palvelu vai ei.

Porttiskannaus hyödyntää TCP protokollan kolmitiekättelyä. Kolmitiekättelyssä yhteyttä avaava laite lähettää kohdelaitteelle SYN-paketin. Kohdelaite vastaa tähän SYN/ACK-paketilla. Lopuksi yhteyttä avaava laite lähettää ACK-paketin, jolloin yhteys on muodostettu. Yhteys suljetaan lähettämällä FIN-paketti ja kuittaamalla se ACK-paketilla. Kumpikin osapuoli katkaisee yhteyden erikseen. Haluttu yhteyden muodostus voidaan keskeyttää lähettämällä RST-paketti. [13]

Yksinkertaisin tapa suorittaa porttiskannaus on yrittää avata yhteys haluttuun porttiin, eli suorittaa kolmitiekättely, ja tämän jälkeen sulkea juuri avattu yhteys, eli lähettämällä lopetuspaketit. Jos tiedusteltavassa portissa on jokin palvelu, onnistuu yhteyden avaaminen. Jos tiedusteltavassa portissa ei ole palvelua, ei myöskään yhteyden avaaminen onnistu. Koska yhteyden täysi avaaminen vaatii useiden pakettien vaihtamista, kuluu tässä paljon aikaa sekä avattu yhteys voidaan kirjata lokiin. [14]

Yleisin porttien skannaamiseen käytettävä menetelmä on niin sanottu puoliavoin skannaus. Tällä menetelmällä yhteyden avaaminen aloitetaan lähettämällä SYN-paketti. Jos kohdelaitteessa on tiedusteltava portti auki, vastaa laite SYN/ACK-paketilla. Yhteyttä ei kuitenkaan avata vaan lähettäjä lähettää RST-paketin, jolla ilmaistaan että yhteyden muodostus keskeytetään. Jos tiedusteltavassa portissa ei ole palvelua, vastaa kohdelaite lähettämällä RST-paketin ja yhteyden muodostus keskeytyy. Tällöin ei avata yhteyttä kokonaan sekä lähetetään vähemmän paketteja, jolloin skannaus on nopeampi. Kohde ei myöskään kirjaa yrityksiä ylös, sillä yhteyttä ei avata kokonaan. [14]

Kolmas tapa on hyödyntää TCP-standardissa olevia porsaanreikiä. Tässä lähetetään virheellisiä TCP-paketteja, jolloin kohdelaitteen pitäisi vastata tietyllä tavalla portin ollessa auki tai kiinni. Virheellisten TCP-pakettien lähettäminen mahdollistaa joidenkin tilattomien palomuurien ohittamisen. [14]

Porttiskannaus voidaan suorittaa käyttäen joko tiettyjä valikoituja yleisempiä portteja tai vaihtoehtoisesti voidaan kaikki mahdolliset portit skannata läpi. Porttiskannaus tuottaa listan avoimista porteista. Pelkän porttiskannauksen jälkeen ei vielä tiedetä mitä palveluita kohteessa on. Portissa oleva palvelu voi selvitä pelkän porttinumeron perusteella. Esimerkiksi HTTP-protokollan käyttämä oletusportti on portti numero 80. Palvelu voi kuitenkin toimia jossain muussa portissa kuin sen oletusportissa tai se voi toimia jonkin toisen palvelun oletusportissa. Palvelua ei tästä syystä voi luotettavasti todentaa pelkän porttinumeron perusteella. Palvelun tarkempi selvittäminen vaatii yhteyden muodostamista kyseisen palvelun kanssa. [15]

Porttiskannausta vaikeuttava tekijä on palomuuri. Palomuuri estää liikenteen portteihin joihin ei haluta pääsyä palomuurin ulkopuolelta. Palomuureja on kahta päätyyppiä, tilattomia ja tilallisia. Tilattomat palomuurit eivät pidä yllä tietoa palomuurin läpikulkevista paketeista. Tilalliset palomuurit taas pitävät tietoa palomuurin läpi muodostetuista yhteyksistä ja sallivat vain liikenteen joka on osa muodostettua yhteyttä. [16] Tilattomat palomuurit estävät yhteyden muodostamisen estettyyn porttiin, mutta voivat päästää muuta liikennettä, kuten epämääräisiä TCP-paketteja läpi [14].

3.3 Haavoittuvuuksien selvittäminen

Verkon skannaamisen jälkeen hyökkääjällä on tiedossa kohdejärjestelmän aktiivilaitteet ja niiden tarjoamat palvelut. Haavoittuvuuksien selvittäminen on hyökkääjän seuraava vaihe verkon skannaamisen jälkeen ja voi tapahtua myös samanaikaisesti muun verkon skannaamisen kanssa. Selvittämällä kohteen tietojärjestelmien haavoittuvuudet, voi hyökkääjä löytää mahdollisen reitin kohteen tietojärjestelmiin. [1, s. 84] Haavoittuvuus on tietojärjestelmässä oleva heikkous, joka mahdollistaa tietojärjestelmään tunkeutumisen. Haavoittuvuuksien syinä voivat olla esimerkiksi ohjelmiston suunnitteluvirheet, ohjelmointivirheet tai käyttäjän syöttämän tiedon tarkistamatta jättäminen [17]. Myös väärin asennetut palvelut voivat olla haavoittuvaisia [1, s. 84].

3.3.1 Version tunnistus

Ohjelmiston versionumerosta voidaan päätellä, onko käytössä oleva versio uusin versio vai onko käytössä vanhentunut versio, joka voi sisältää tunnettuja haavoittuvuuksia. Hyökkääjä voi siis ohjelmiston version selvittämisen jälkeen etsiä mahdollisia haavoittuvuuksia juuri kyseisestä ohjelmistoversiosta.

Palvelu ja sen versio voidaan tunnistaa hyödyntämällä tietoa sen käyttämästä porttinumerosta. Esimerkiksi www-palvelimen oletusportti on portti 80. Tällöin portista 80 löydetty palvelu voidaan määrittää www-palvelimeksi. Ongelma muodostuu siitä, ettei palveluita ole pakotettu käyttämään tiettyä porttia, vaan palvelu voi käyttää mitä tahansa porttia. Esimerkiksi porttia 23 käyttävä telnet-palvelu voi käyttää hyökkääjän hämäämiseksi turvallisemman SSH-palvelun porttia numero 22. Porttiin perustuvan tunnistuksen jälkeen havaittu palvelu tulkitaan olevan paremmin suojattu SSH-palvelin vaikka se todellisuudessa onkin suojaamaton telnet. [1, s. 85; 15]

Varmempi tunnistus saadaan seuraamalla palvelun ”tunnuksia” (banner). Palvelut voivat kertoa itsestään lähettämällä ”tunnuksen”, jossa on tiedot palvelusta, kuten palvelun nimi ja versionumero. Tietyt palvelut lähettävät oman ”tunnuksensa” kun niihin avataan yhteys. Toiset ilmoittavat oman tunnuksensa kun niille lähettää oikein muotoillun komennon tai virheellisen komennon. Tällöin palvelun käyttämällä portilla ei ole mitään väliä, sillä palvelun tunnistaminen tehdään hyödyntämällä palvelun vastausta. Tämän menetelmän käyttäminen kuitenkin vaatii yhteyden muodostamista haluttuun porttiin, josta jää jälki palvelimelle ja hyökkääjä voi paljastua. [1, s. 85; 15]

3.3.2 Haavoittuvuusskannaus

Haavoittuvuusskannauksella etsitään tietojärjestelmistä haavoittuvuuksia tätä tarkoitusta varten tehdyillä ohjelmilla. Haavoittuvuusskannaukseen tarkoitettuja ohjelmia kuten Nessus tai OpenVAS, käytetään järjestelmien turvallisuuden tutkimiseen käytetyssä penetraatiotestauksessa. Samoja ohjelmia voidaan kuitenkin käyttää myös varsinaiseen järjestelmään tunkeutumiseen[11, s. 55].

Haavoittuvuusskannauksessa hyödynnetään tietoa tunnetuista haavoittuvuuksista, joita ohjelma testaa porttiskannauksella löydettyihin portteihin. Menetelmä on aiheuttaa todennäköisesti paljon huomiota. Hyökkääjä käyttää haavoittuvuusskannausta, jos hyökkääjä tietää ettei kohteella ole kunnollista suojausta sitä vastaan, tai hyökkääjällä on tarve toimia nopeasti, eikä paljastumisella ole väliä. Haavoittuvuusskannauksella voidaan saada helposti ja melko nopeasti tiedot jonkin tietojärjestelmän haavoittuvuuksista. [1, s. 87]

Haavoittuvuusskannauksessa käytetään hyödyksi porttiskannauksessa saatuja tuloksia. Haavoittuvuusskannaukseen käytetyissä ohjelmissa onkin porttiskannauksen suorittava komponentti, ja skannaus aloitetaan suorittamalla porttiskannaus kuten aikaisemmin on kerrottu. Porttiskannauksen jälkeen tiedossa on kohteessa avoinna olevat portit sekä mahdollisesti tieto niissä olevista palveluista ja niiden versioista. Haavoittuvuusskannaukseen tarkoitetut työkalut, kuten Nessus, yrittävät hyökätä avoinna olevissa porteissa oleviin palveluihin käyttämällä tunnettuja haavoittuvuuksia. Palvelun reaktiosta voidaan päätellä toimiiko kyseinen haavoittuvuus kyseistä palvelua vastaan vai onko järjestelmässä mahdollisesti käytössä korjattu ohjelmaversio kyseisestä palvelusta. Haavoittuvuuden löytyminen tai haavoittuvuuden toimimattomuus kertoo myös tarkemmin käytössä olevan ohjelmistoversion.

4 JOHTOPÄÄTÖKSET

Verkkotiedustelu on ennen verkkohyökkäystä tapahtuvaa tiedustelua. Tiedustelun toimintaan vaikuttaa tiedusteltava kohde. Tutkielmassa esiteltiin kaksi erilaista kohdetta. Kohdistettu hyökkäys kohdistuu kohteen hallussa pitämään tietoon, kun taas erilaiset automaatiojärjestelmät mahdollistavat fyysisen maailman toimintojen, kuten kriittisen infrastruktuurin, hallitsemisen.

Kriittisen infrastruktuurin ja automaatiolaitteiden tapauksessa hyökkääjän täytyy ensin löytää haluamansa kohde. Tähän hyökkääjällä on apuna erilaiset hakukoneet kuten Shodan, jolla hyökkääjä voi helposti etsiä esimerkiksi tietyn tyyppisiä automaatiolaitteita tietystä valtiosta. Hyökkääjä voi toisaalta tehdä myös koko Internetin tai yksittäisen valtion IP-osoitteet kattavan porttiskannauksen haluamistaan porteista. Kaikkia Internetiin yhteydessä olevia automaatiolaitteita ei ole suojattu tarpeeksi hyvin, mikä mahdollistaan niiden luvattoman käyttämisen. Automaatiolaitteiden tietoturvassa ei myöskään pidä luottaa järjestelmien ainutlaatuisuuteen, sillä hyökkääjä voi saada haltuunsa järjestelmän tiedot muita reittejä pitkin. Kuvitellaan tilanne, jossa hyökkääjä haluaa päästä käyttämään kohteen automaatiojärjestelmää. Järjestelmä voi olla vain kyseiseen käyttötarkoitukseen rakennettu, eikä sitä ole käytössä muualla. Hyökkääjä pystyy selvittämään järjestelmän toimittaneen organisaation ja suorittaa kohdistetun hyökkäyksen järjestelmän toimittajaa vastaan. Hyökkääjä saa tällöin haluamansa tiedot oikeasta kohteestaan ja voi jatkaa hyökkäystä varsinaista kohdetta vastaan.

Verkkohyökkäyksen ja samalla verkkotiedustelun kohteena voi siis olla mikä tahansa organisaatio, jolla on jotain hyökkääjän haluamaa tietoa tai kohteeseen hyökkäämällä hyökkääjä saavuttaa jonkin muun päämäärän. Tällöin kohteen uhkana on kohdistettu hyökkäys, joka voi kestää pitkään ennen sen paljastumista. Se voi toisaalta olla myös nopea, jolloin hyökkääjä poistuu kohteesta kun on saanut tehtävänsä suoritettua. Kohdistettu hyökkäys voidaan toteuttaa myös käyttäen haittaohjelmia, jotka järjestelmään päästyään etsivät hyökkääjän haluamat tiedot ja lähettävät ne hyökkääjälle. Kohdistetussa hyökkäyksessä verkkotiedustelu todennäköisesti etenee tutkielmassa kuvattujen kolmen vaiheen kautta.

		Käyttötarkoitus	Saatavilla oleva tieto	Tiedon vaikutus	Havaittavuus
Julkiset lähteet	Verkkosivut	Hyökkäyksen tiedustelu	Kohteen henkilöt Kohteen hankkeet Kohteen verkon tekniikka	Mahdollistaa hyökkäyksen kohdistamisen	Ei eroa normaalista verkkoliikenteestä
	DNS	Hyökkäyksen tiedustelu	Zone transfer voi palauttaa kaiken tiedon nimipalvelimelta.	Kertoo paljon verkon rakenteesta.	Ei kohteen havaittavissa.
	WHOIS	Hyökkäyksen tiedustelu	Kohteen nimipalvelimet ja verkko-osoitteet. Ylläpitäjien yhteystietoja	Kertoo verkon rakenteesta. Mahdollistaa hyökkäyksen kohdistamisen.	Ei kohteen havaittavissa
	Yleishakukoneet	Hyökkäyksen tiedustelu Kohteen etsintä	Perustiedot kohteesta. Verkkolaitteiden tiedot	Mahdollistaa hyökkäyksen kohdistamisen. Kertoo verkon rakenteesta	Ei kohteen havaittavissa
	Shodan	Kohteen etsintä	Internetiin yhteydessä olevat laitteet	Mahdollistaa hyökkäykselle alttiiden kohteiden etsinnän Internetistä	Ei kohteen havaittavissa
Verkon skannaaminen	Ping-skannaus	Hyökkäyksen tiedustelu.	Kohteen aktiiviset verkkolaitteet	Kertoo verkon rakenteesta. Mahdollistaa tiedustelun kohdistamisen vain aktiivisiin laitteisiin	Ping-kysely normaalia verkkoliikennettä. Verkon skannaus havaittavissa verkkoliikenteestä.
	Porttiskannaus	Hyökkäyksen tiedustelu. Kohteen etsintä.	Verkon laitteiden tarjoamat palvelut	Havaitut palvelut ovat mahdollisia hyökkäysreittejä	Skannaus on epäilyttävää verkkoliikennettä
Haavoittuvuuksien selvittäminen	Version tunnistus	Hyökkäyksen tiedustelu. Kohteen etsintä.	Palvelun tyyppi ja palvelun versio	Versionumeron perusteella voidaan etsiä haavoittuvuuksia	Ei eroa juurikaan tavallisesta liikenteestä. Voidaan suorittaa porttiskannauksen yhteydessä, jolloin aiheuttaa havaittavaa verkkoliikennettä
	Haavoittuvuusskannaus	Hyökkäyksen tiedustelu	Verkon palveluissa olevat tunnetut haavoittuvuudet.	Löytynyt haavoittuvuus mahdollistaa hyökkäämisen järjestelmään haavoittuvuuden kautta	Rinnastettavissa murron yrittämiseen. Aiheuttaa hyvin paljon epätavallista toimintaa.

Taulukko 1 Verkkotiedustelun menetelmät

Tutkimuksessa käsitellyt verkkotiedustelussa käytettävät menetelmät on tiivistetty taulukkoon 1. Taulukko on järjestetty tiedustelun vaiheiden mukaisesti. Tiedustelu aloitetaan tutkimalla julkisesti saatavilla olevaa informaatiota. Tutkimuksessa käsiteltyjä julkisia lähteitä ovat kohteen ja sen yhteistyöorganisaatioiden verkkosivut, DNS- ja WHOIS-palvelut, hakukoneet ja Shodan. Koska kaikki julkisista lähteistä saatava tieto ei ole kohteen hallitsemaa, on saatavilla olevan tiedon määrää vaikea rajoittaa. Tiedustelun toisessa vaiheessa käytetään erilaisia skannausmenetelmiä ja selvitetään verkossa olevia palveluja esimerkiksi porttiskannauksella. Kolmannessa vaiheessa selvitetään löydetyistä palveluista varsinaisen hyökkäyksen suorittamiseen tarvittavat haavoittuvuudet tunnistamalla palveluiden versiot tai käyttämällä haavoittuvuusskannausta.

Käsitellystä menetelmästä kerrotaan menetelmän avulla saatava tieto sekä tiedon vaikutukset. Esimerkiksi WHOIS-palvelun kautta on mahdollista saada tietoa kohteen verkko-osoitteista ja nimipalvelimista, jotka kertovat hyökkääjälle verkon rakenteesta, sekä ylläpitäjien yhteystietoja, jotka mahdollistavat hyökkäyksen kohdentamisen. Verkon skannausmenetelmillä saadaan enemmän tietoa kohteen verkosta ja niillä voi paljastaa murrettavia palveluita.

Menetelmän käyttötarkoituksella kuvataan käytetäänkö menetelmää hyökkäystä edeltävässä tiedustelussa vai soveltuuko menetelmä käytettäväksi uusien hyökättävien kohteiden etsintään. Kohteen verkkosivujen tutkimista käytetään kohteeseen hyökkäämistä edeltävässä tiedustelussa. Hakukone Shodania voidaan käyttää uusien hyökkäykselle alttiiden kohteiden löytämiseen Internetistä. Porttiskannaus soveltuu kumpaankin käyttötarkoitukseen. Porttiskannausta voidaan käyttää hyökkäykseen liittyvässä tiedustelussa verkon palveluiden selvittämiseen, mutta toisaalta esimerkiksi Shodanin tiedot perustuvat koko Internetin käsittäviin porttiskannauksiin, jolloin porttiskannausta voidaan käyttää myös haavoittuvien kohteiden etsintään. Halutun kohteen löytymisen jälkeen voidaan kohdetta vastaan aloitta tiedustelu hyödyntäen hyökkäyksen tiedusteluun soveltuvia menetelmiä.

Taulukossa on myös käsitelty käytettävän menetelmän aiheuttamaa huomiota. Taulukosta huomaa, että aluksi julkisia lähteitä käyttämällä tiedot saadaan helposti paljastumatta, mutta verkon skannaamisessa käytettävät menetelmät aiheuttavat enemmän tavallisesta poikkeavaa verkkoliikennettä. Kohteen verkkosivuilta tapahtuva tiedon kerääminen ei eroa normaalista verkkoliikenteestä, joten sen havaitseminen on vaikeaa. Verkon skannaamisessa ei yksittäinen yhteyden avaus todennäköisesti vaikuta tavanomaisesta poikkeavalta, mutta kaikkien porttien ja verkon aktiivilaitteiden skannaaminen on jo hyvin epätavallista ja voi paljastaa hyökkääjän. Haavoittuvuusskannaus, jossa hyökkääjä kokeilee haavoittuvuuksien toimintaa havaittuihin palveluihin voi vaikuttaa jopa äänekkäältä murrolta kohteeseen.

Verkkotiedustelu on yksinkertaistettuna hyökättävän kohteen etsimistä. Etsiminen voi kohdistua uuden kohteen löytämiseen tai se voi kohdistua tiedon hankkimiseen löydetystä kohteesta. Päätavoitteena kuitenkin on järjestelmään murtautumisen mahdollistaminen. Tiedustelu alkaa laajasti keräämällä mahdollisimman paljon tietoa kohteesta ja päättyy yhteen tai useampaan pisteeseen, joista murto kohteeseen on mahdollista. Hyvin suoritetun tiedustelun jälkeen hyökkääjän on mahdollista suorittaa oma tehtävänsä kohteessa, eikä kohde havaitse hyökkäystä ennen kuin on liian myöhäistä.

LÄHTEET

[1] McClure S., Scambray J. & Kurtz G. *Hacking Exposed 7: network security secrets & solutions*, Yhdysvallat: McGraw-Hill, 2012, 741 s. ISBN 978-0-07-178028-5

[2] Thion R. *Network-Based Passive Information Gathering*. In: Janczewski L.J. & Colarik A.M. (eds.) Cyber warfare and cyber terrorism. Yhdysvallat: IGI Global, 2008, 532 s. ISBN 978-1-59140-991-5

[3] Andress, J. & Winterfeld S. *Cyber warfare: techniques, tactics and tools for security practitioners*. Yhdysvallat: Syngress Publishing, 2011, 289 s. ISBN 978-1-59749-637-7

[4] Owen R.S. *Infrastructures of Cyber Warfare*. In: Janczewski L.J. & Colarik A.M. (eds.) Cyber warfare and cyber terrorism. Yhdysvallat: IGI Global, 2008, 532 s. ISBN 978-1-59140-991-5

[5] CERT-FI, *Kohdistetut haittaohjelmahyökkäykset*. [viitattu 8.11.2013]. Saatavissa: http://www.cert.fi/tietoturvanyt/2013/11/ttn201311011336.html

[6] *Kohdistetut hyökkäykset*. Valtiovarainministeriö. 2009. ISSN 978-952-251-013-6. [viitattu: 2.8.2013]. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20091117Kohdis/kohdistetut_hyoekkaeykset_netti_kannet.pdf

[7] Kiravuo T. *Offensive Cyber-capabilities against Critical Infrastructure*. In: Vankka J. (ed.) *Cyber Warfare*. Tampere: Juvenes Print. 2013. 127 s. ISBN 978-951-25-2456-3

[8] Ekman J. *Tunkeutumisenesto ja havainnointi käytönvalvontajärjestelmissä*. Opinnäytetyö, Helsinki, 2009, Metropolia, Tietotekniikan koulutusohjelma, 52 s.

[9] Rantapelkonen J. & Salminen M. *The fog of cyber defence*, Tampere: Juvenes Print Oy, 2013, 234 s. ISBN 978–951–25–2431–0

[10] Tiilikainen, S., Manner J. *Suomen automaatioverkkojen haavoittuvuus*. Helsinki, 2013, Aalto-yliopisto

[11] Pullinen M. *Kriittisten tietojärjestelmien suojaaminen kyberuhilta*. Opinnäytetyö, Leppävaara, 2012, Laurea-ammattikorkeakoulu, Tietojenkäsittelyn koulutusohjelma YAMK, 86 s.

[12] Network Uptime. *Secrets of Network Cartography - Ping Scan (-sP)*. [viitattu 15.1.2014]. Saatavissa: http://www.networkuptime.com/nmap/page3-8.shtml

[13] Wikipedia. *TCP*. [viitattu 15.1.2014]. Saatavissa: http://fi.wikipedia.org/wiki/TCP

[14] Nmap. *Port Scanning Techniques*. [viitattu 15.1.2014]. Saatavissa: http://nmap.org/book/man-port-scanning-techniques.html

[15] Nmap. *Service and Version Detection*. [viitattu 15.1.2014]. Saatavissa: http://nmap.org/book/man-version-detection.html

[16] Wikipedia. *Firewall (computing)*. [viitattu 10.3.2014]. Saatavissa: http://en.wikipedia.org/wiki/Firewall_(computing)

[17] Wikipedia. *Vulnerability (computing)*. [viitattu 24.2.2014]. Saatavissa: http://en.wikipedia.org/wiki/Vulnerability_(computing)