Opinnäytetyö AMK

Tietojenkäsittely

2019

Aarni Roininen

SCADA/ICS-VERKKOJEN TIETOTURVAONGELMAT JA KORJAUSTOIMENPITEET

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ AMK | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2019 | 47 sivua

Aarni Roininen

SCADA/ICS-VERKKOJEN TIETOTURVAONGELMAT JA KORJAUSTOIMENPITEET

Opinnäytetyön tarkoituksena oli kerätä tietoa tuotanto- ja teollisuusverkkoihin liittyvistä tietoturvaongelmista, testata niiden tietoturvaa käytännössä sekä koostaa tietoturvakontrolleja verkkojen tietoturvaongelmien lieventämiseksi.

Opinnäytetyö käsitteli tuotanto- ja teollisuusverkkojen toimintaa yleisellä tasolla ja kävi läpi teollisuusverkoissa eniten käytettyjä protokollia, kuten Modbus, DNP3, IEC 60870-5-140, sekä niissä verkoissa laajalti käytettyjä PLC-, RTU- ja HMI-komponentteja.

Lisäksi opinnäytetyössä käytiin läpi tunnettuja hyökkäyksiä tuotanto- ja teollisuusverkkoja vastaan sekä simuloitiin hyökkäys virtuaaliympäristössä. Osana opinnäytetyötä kerättiin myös oikeaa hyökkäysliikennettä PLC-komponentteja esittävillä palvelimilla. Palvelimilla kerättiin erityisesti tietoa hyökkäyksien määrästä.

Kerätyn tiedon sekä suoritettujen testien perusteella koostettiin tietoturvakontrolleja, joilla yleisimpiä haavoittuvuuksia voidaan korjata tai niiden vaikutuksia voidaan lieventää.

ASIASANAT:

Tuotantoverkko, teollisuusverkko, verkkoprotokolla, penetraatiotestaus, tietoturvakontrollit

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology

2019 | 47 pages

Aarni Roininen

SCADA/ICS NETWORK SECURITY, THREATS AND MITIGATIONS

The purpose of this thesis was to gather information related to SCADA/ICS network security, to test SCADA/ICS network environment and to produce security controls to mitigate the impact of security issues.

This thesis goes through how SCADA/ICS network functions, the most used protocols, such as Modbus, DNP3, IEC 60870-5-140 and commonly used components such as PLC, RTU and HMI.

Also, this thesis includes information on some known attacks against SCADA/ICS networks and simulates an attack against SCADA/ICS network in a virtual environment. As a part of the thesis, real attack data against PLC components is captured and monitored.

At the end, security controls are produced based on the information gathered and the results of the tests performed. These security controls focus on fixing the vulnerabilities and mitigating the risks.

KEYWORDS:

SCADA, ICS, network protocol, penetration testing, security controls

SISÄLTÖ

KUVAT

SANASTO

ARP	Address Resolution Protocol selvittää verkkolaitteiden fyysisen osoitteen
BinaryEdge	Hakukone, jonka kautta voi hakea verkkoon yhdistettyjä laitteita
Black Box	Penetraatiotestaustapa, jossa ei tiedetä kohteesta mitään ennen testauksen aloittamista
Conpot	Tuotanto- ja teollisuusjärjestelmiä esittävä hunajapurkkiohjelmisto
Denial of Service	Palvelunestohyökkäys, joka estää järjestelmän käytön kokonaan
DNP3	Distributed Network Protocol, tuotanto- ja teollisuusympäristöissä laajasti käytetty verkkoprotolla, jolla voidaan valvoa laitteiden tai tuotantoprosessien toimintaa
Docker	Kevyt ja nopea virtuaaliympäristö
EC2	Amazon Elastic Compute Cloud, pilvipalvelu, josta voi vuokrata palvelintilaa
Gray Box	Black Box ja White Box menetelmiä yhdistävä penetraatiotestauksen menetelmä
HMI	Human Machine Interface, on laite, joka tarjoaa ihmisille rajapinnan kommunikoida sekä monitoroida järjestelmän kanssa
Honeypot	Hunajapurkki eli ansajärjestelmä, joka esittää oikeaa järjestelmää
HoneyScore	Shodan hakukoneen käyttämä tarkistustyökalu, joka pyrkii tunnistamaan hunajapurkkeja
HTTP	Hypertext Transfer Protocol, on verkkoliikenne protokolla

ICS	Industrial Control System, teollisuusautomaatiojärjestelmä
IEC	International Electrotechnical Commission, on kansainvälinen standardien julkaisujärjestö
IEC 60870-5	Tuotanto- ja teollisuusympäristöissä laajasti käytetty verkkoprotokolla, jolla voidaan valvoa laitteiden tai tuotantoprosessien toimintaa
Man in the Middle	Välimieshyökkäys, jossa hyökkääjä onnistuu kuuntelemaan ja muokkaamaan liikennettä
Master/Slave	Pää- sekä ala-asemakonfiguraatio, jossa pääasema ohjaa ala-asemaa
Modbus	Tuotanto- ja teollisuusjärjestelmissä laajasti käytössä oleva verkkoprotokolla, jolla voidaan valvoa laitteiden tai tuotantoprosessin toimintaa
Nmap	Network Mapper on verkkojen skannaukseen käytetty työkalu
PLC	Logiikkakontrolleri, joka tekee toimintoja sensoreilta saadun tiedon perusteella
RTU	Remote Terminal Unit, on etäpäätelaite, joka kerää ja välittää tietoa kentältä ohjauskeskukselle
SCADA	Supervisory Control and Data Acquisition eli monitorointi- sekä tiedonkeräysjärjestelmä
Shodan	Verkkoon liitettyjen laitteiden hakukone
SSH	Secure Shell on verkkoprotokolla etälaitteiden hallintaan
TCP/IP	Transmission Control Protocol / Internet Protcol ovat verkkoliikenteen standardit
White box	Järjestelmän testausmenetelmä, jossa testaajalla on tietoa järjestelmän toiminnasta

1 JOHDANTO

Tuotanto- ja teollisuusverkkoja (engl. SCADA/ICS networks) on ollut käytössä jo pitkään. Ne ovat osa yhteiskunnan kriittisiä toimintoja, ja niitä käytetään laajasti erilaisissa prosessien ohjaus-, monitorointi- sekä automaatiojärjestelmissä. Kyseiset verkot ovat tärkeä osa yhteiskunnan infrastruktuuria (Stouffer ym. 2015, 17), sillä tuotanto- ja teollisuusverkkoja on käytössä muun muassa ydinvoimaloissa, vedenpuhdistamoissa, sähkönjakelussa ja kiinteistöautomaatiossa.

Näiden verkkojen toimintavarmuus sekä tietoturva ovat erittäin tärkeitä asioita, sillä verkot ohjaavat sekä monitoroivat monia yhteiskunnan normaalille toiminnalle välttämättömien laitoksien järjestelmiä. Tietoturva on yksi verkkojen toimintavarmuuteen vaikuttavista asioista, ja se on nousemassa koko ajan tärkeämpään rooliin tuotanto- ja teollisuusverkkojen toimintavarmuuden takaamisessa. Laitoksia ja niiden tietojärjestelmiä kytketään jatkuvasti enenevissä määrin julkisesta verkosta saavutettaviksi, jolloin tietoturvan rooli korostuu (Stouffer ym. 2015, 16).

Laitoksien yhteydet internetin yli mahdollistavat uusien ominaisuuksien ja toiminnallisuuksien lisäämisen, joka taas helpottaa jo olemassa olevien prosessien valvontaa ja ohjaamista. Internetyhteydet kuitenkin altistavat uusille hyökkäyksille, joilla pyritään häiritsemään ja mahdollisesti jopa pysäyttämään laitoksen toiminnan jatkuvuudelle kriittisiä prosesseja.

Vaikka laitoksen omaan verkkoon ei olisi ollenkaan pääsyä internetistä, täytyy jo käytössä olevien tuotanto- ja teollisuusverkkojen tietoturvaan silti kiinnittää huomiota. Motivoitunut hyökkääjä, joka on suunnitellut kohdistetun hyökkäyksen järjestelmää vastaan, ei välttämättä tarvitse verkkoyhteyttä ulkoverkon kautta tuotanto- tai teollisuusverkkoon kohdistuvan hyökkäyksen suorittamiseksi. Laitoksen käytössä olevat verkkoprotokollat ja komponentit ovat tällöin suoraa hyökkäyksen kohteina, ja jos niiden tietoturvaan ei ole panostettu, on tuotantoprosesseihin mahdollista päästä vaikuttamaan. Fyysinen tietoturvan sekä laitoksen sisäverkon tietoturvan tulisi olla kunnossa, mutta myös tuotanto- tai teollisuusverkon tietoturvan taso on tällöin avainasemassa. Monikerroksinen puolustus perustuu niin sanottuun ”Defense in Depth” -strategiaan (Barnum ym. 2005).

Alun perin tuotanto- ja teollisuusverkoissa tietoturvaa ei huomioitu ollenkaan, mutta ajan kuluessa myös tietoturva on otettu osaksi verkoissa käytettävien protokollien ja

komponenttien kehitystä. Kehitystä tähän suuntaan on ajanut muiden tietoturvaa parantavien protokollien kehitys sekä laitosten laajemmat verkkoyhteydet, jotka altistavat tuotanto- ja teollisuusverkkoja hyökkäyksille. Tuotanto- ja teollisuusverkkojen suurimpia puutteita ovat edelleen hyvin perustavanlaatuiset ongelmat, kuten salaamattomat yhteydet ja autentikointi. Laitoksissa käytettyjen protokollien ja komponenttien kehitys on tietoturvan näkökulmasta muiden verkkoprotokollien ja laitteiden kehitystä jäljessä.

Toimintavarmuuden takaaminen esimerkiksi riskienhallinnan sekä ”Defense in Depth” -strategian (Barnum ym. 2005) keinoin ovat isossa osassa tämän hetken tuotanto-, ja teollisuusverkkoympäristöjä, sillä käytössä olevat protokollat eivät välttämättä ole tietoturvallisia tai niitä ei ole edes mahdollista päivittää turvallisempiin versioihin. Myös suorittamalla tietoturvatestauksia järjestelmiä kohtaan ja parantamalla tunnistettuja heikkoja kohtia, voidaan riskejä pienentää. Ajantasaiset tietoturvakontrollit ja tietoturvapolitiikat, joita noudatetaan osana laitoksen arkea, tuovat myös lisäkerroksen tietoturvaa ja tukevat paremman toimintavarmuuden saavuttamista.

2 TUOTANTO- JA TEOLLISUUSVERKOT JA VERKKOPROTOKOLLAT

2.1 Tuotanto- ja teollisuusverkot

SCADA (Supervisory Control and Data Acquisition) -verkot eli tuotanto- ja teollisuusverkot ovat laajassa käytössä monitorointia ja ohjausta vaativissa järjestelmissä. Tällaiset järjestelmät usein kattavat laajoja alueita, jolloin järjestelmän monitorointi ja ohjaaminen voi tapahtua kaukana itse tuotantolaitoksesta. Tuotanto- ja teollisuusverkot koostuvat useista eri osista, joita ovat erilaiset verkkolaitteet sekä näiden verkkolaitteiden välisessä kommunikaatiossa käytetyt protokollat.

Tuotanto- ja teollisuusverkkojen tarkoituksena on kerätä tietoa tuotantoympäristön toiminnasta, ja siten mahdollistaa tuotantoympäristön toiminnan reaaliaikainen monitorointi (Bailey & Wright 2003, 2). Tuotantoympäristön laitteita, esimerkiksi pumppuja tai moottoreita voidaan myös ohjata verkon avulla tilanteen vaatimalla tavalla.

Tuotanto- ja teollisuusverkot koostuvat esimerkiksi sensoreista, jotka keräävät reaaliaikaista tietoa tuotantoympäristön toiminnasta. Kerättyä tietoa voi olla esimerkiksi veden lämpötila, moottorin pyörimisnopeus tai akun varauksen taso. Nämä laitteet lähettävät niiden keräämää tietoa eteenpäin seuraavalle laitteelle. (Bailey & Wright 2003, 12)

2.1.1 Etäpäätelaite (RTU)

Yksinkertaisessa verkkoympäristössä seuraava laite on etäpäätelaite eli RTU (Remote Terminal Unit), joka monitoroi sekä kontrolloi verkon laitteita (Stouffer ym. 2015, 131). Etäpäätelaitteen ja tietoa keräävän sensorin välissä voi olla erillinen logiikkakontrolleri tai etäpäätelaite sekä logiikkakontrolleri voivat olla sama laite, joka hoitaa molempien virkoja. Etäpäätelaite ja logiikkakontrolleri eivät välttämättä eroa toisistaan paljoa ja siksi niiden yhdistäminen on kustannustehokasta.

Etäpäätelaitteen tehtävä on kerätä sensorien ja mittarien lähettämää tietoa ja välittää tietoa eteenpäin ohjauskeskukseen. Etäpäätelaite voi myös kommunikoida järjestelmän muiden etäpäätelaitteiden kanssa ja yksi laite voi vastaanottaa liikennettä muilta vastaavilta laitteilta ja lähettää sen eteenpäin niiden puolesta, eli toimia liikenteen välittäjänä

(Bailey & Wright 2003, 17–18). Etäpäätelaitteen käyttäminen välittäjänä on hyödyllistä etenkin, jos tietty etäpäätelaite ei ole suoraan ohjauskeskuksen saavutettavissa.

2.1.2 Logiikkakontrolleri (PLC)

Useissa tuotanto- ja teollisuusverkoissa käytetään logiikkakontrollereita eli PLC (Programmable Logic Controller) -laitteita, jotka tekevät sensorien ja mittarien keräämään tiedon perusteella päätöksiä mitä toimenpiteitä tulee suorittaa seuraavaksi (Stouffer ym. 2015, 130). Nämä laitteet ovat siis tuotantoympäristöön sijoitettuja ohjauslaitteita.

Logiikkakontrollerit ovat usein edullisempia kuin erilliset etäpäätelaitteet ja niitä suositaan niiden muokattavuuden ja toimintavarmuuden vuoksi. Logiikkakontrollereita voidaan käyttää monessa tarkoituksessa ja ne ovatkin siirtäneet tuotanto- ja teollisuusverkkojen painopistettä erilaisista fyysisistä osista ohjelmistoihin. Ohjelmistopainotteinen verkko mahdollistaa helpomman vikatilanteiden selvittämisen verkossa ja verkkolaitteissa. (Bailey & Wright 2003, 37)

Jos hyökkäävä taho pääsee muuttamaan logiikkakontrolleriin ohjelmoitua logiikkaa, voi sen avulla häiritä järjestelmän toimintaa. Logiikkakontrollerin fyysinen turvallisuus tulisi siis varmistaa. Fyysisen turvallisuuden takaaminen voi kuitenkin olla hankalaa, sillä logiikkakontrolleri voi olla sijoitettuna miehittämättömälle laitokselle.

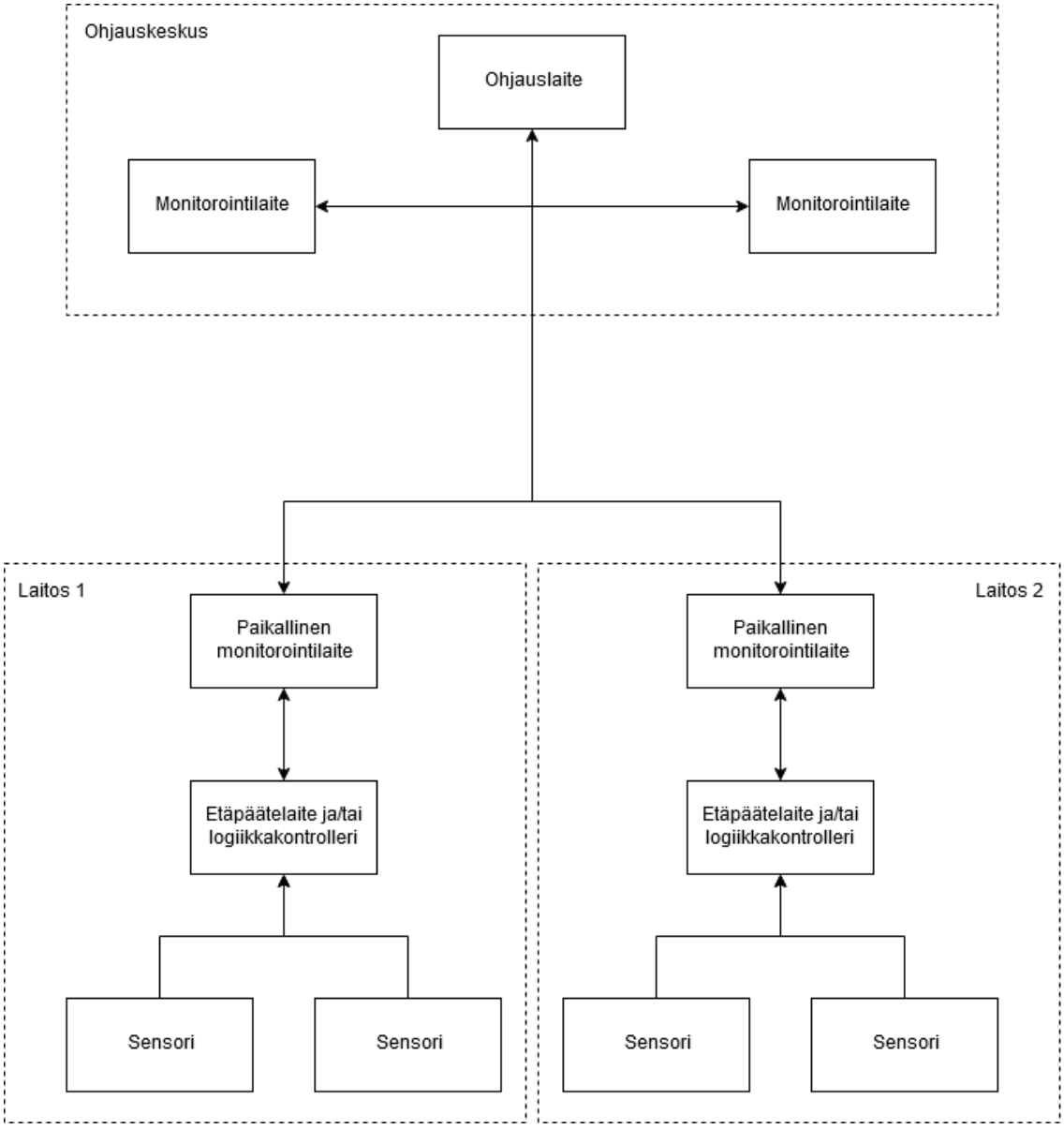
2.1.3 Monitorointi- ja ohjauslaite (HMI)

Monitorointi- ja ohjauslaitteet eli HMI (Human Machine Interface) -laitteet ovat tietokoneita, jotka saavat tietoa kentällä olevilta sensoreilta ja näyttävät sen ihmisen ymmärrettävässä muodossa (Stouffer ym. 2015, 125).

Osa HMI-laitteista on vain monitorointilaitteita ja ohjauslaitteet on sijoitettu vain turvallisiin tiloihin, kuten ohjauskeskukseen. Monitorointi laitteita voi olla kentällä ja niiden kautta voidaan seurata verkon toimintaa ja hälytyksiä paikan päällä, mutta niiden kautta ei voida ohjata tai muokata verkon tai verkkolaitteiden toimintaa.

Paikallisten monitorointilaitteiden kautta ei myöskään tulisi olla pääsyä ohjauskeskuksen verkkoon, vaikka laitoksen ja ohjauskeskuksen välillä onkin yhteys. Verkon segmentointi yleisestikin on iso tekijä tuotanto- ja teollisuusverkkojen yleisen tietoturvan

rakentamisessa (Stouffer ym. 2015, 61). Kuvassa 1 on mallinnettu verkkokaavio yksinkertaisesta tuotanto- tai teollisuusverkosta, joka sisältää kaksi erillistä laitosta.



Kuva 1. Yksinkertainen tuotanto- tai teollisuusverkko.

2.2 Yleisiä tuotanto- ja teollisuusverkkojen protokollia

Tuotanto- ja teollisuusverkoissa voidaan käyttää useita erilaisia protokollia. Eri protokollat ovat eri tahojen kehittämiä, erilaisiin tarkoituksiin. Protokollat saattavat myös olla patentoituja ja niiden käytöstä tulee maksaa. Toiset protokollat saattavat olla täysin avoimia

ja ne mahdollistavat protokollien edullisemman käyttöönoton. Avoimet ja standardoidut protokollat ovatkin saavuttaneet suuren suosion juuri niiden laajan yhteensopivuuden eri laitevalmistajien kanssa sekä ilmaisen käyttöönoton vuoksi.

Erilaiset protokollat ovat usein tarkoitettu hieman erilaisiin käyttötarkoituksiin. Tuotanto- ja teollisuusjärjestelmissä on usein kuitenkin mahdollista käyttää samoja protokollia useissa erilaisissa laitoksissa. Jotkut tuotanto- ja teollisuusverkkojen käyttöön kehitetyt protokollat ovat yleistyneet toisia enemmän tietyillä maantieteellisillä alueilla, mutta myös tietyn tyyppisten laitoksien käytössä. (Clarke ym. 2004, 66)

2.2.1 Modbus

Modbus on yksi käytetyimmistä tuotanto- ja teollisuusverkkoprotokollista ja se on täysin avoin standardi. Avoimuuden ansiosta on Modbus ollut helppo ottaa käyttöön, ja se on ollut edullinen vaihtoehto, sillä protokollasta ei tarvitse maksaa lisenssimaksuja.

Modbus-protokolla tukee nykyään myös TCP/IP-liikennettä ja siten protokolla on pysynyt ajan tuomien vaatimusten ja kehityksen tasalla. Verkossa olevat laitteet ovat pää- sekä ala-asemia (engl. master and slave), riippuen niiden tarkoituksesta.

Vain pääasemat voivat aloittaa kommunikaation muiden asemien kanssa, ala-asemat vain vastaavat tai suorittavat toiminnon, riippuen pääasemalta saadun viestin sisällöstä. Ala-asemat eivät voi aloittaa kommunikoimaan toisten pää- tai ala-asemien kanssa. (Modbus Organization 2012)

2.2.2 DNP3

DNP3 (Distributed Network Protocol Version 3.3) on nykyään avoin protokollastandardi ja sen ovat ottaneet käyttöön monet laitevalmistajat. (Clarke ym. 2004, 66) Avoimen standardin käyttäminen mahdollistaa eri laitevalmistajien välisten laitteiden yhteensopivuuden. Yhteensopivuus helpottaa laitehankintoja järjestelmän rakennus- sekä ylläpitovaiheessa.

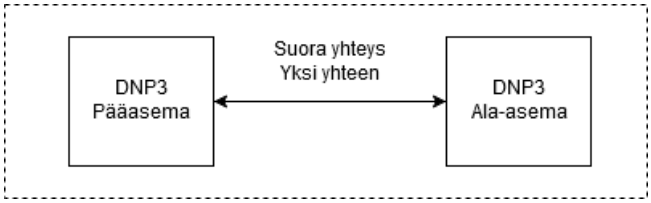
DNP3 on laajasti käytössä sähkö-, öljy-, kaasu- sekä vesilaitoksissa ja sitä tukevia laitteita on paljon. Esimerkiksi useiden laitevalmistajien etäpäätelaitteet tukevat DNP3-protokollaa, joka helpottaa selvästi verkkolaitteiden vaihtamista vikatilanteessa tai

päivityksen yhteydessä. Jos DNP3-protokollaa tukeva laite kykenee lähettämään liikennettä TCP/IP-verkon yli, voidaan DNP3-liikenne pakata Ethernet-paketin sisälle ja lähettää TCP/IP-verkossa. (Clarke ym. 2004, 71)

DNP3-protokolla käyttää myös pääasemia ja ala-asemia, eli pääasema ohjaa ala-asemaa ja vastaanottaa siltä tietoa vastauksina pääaseman kyselyihin. Protokolla tukee kahta päätoimintamallia, kyselevää ja hiljaista. Näitä malleja yhdistelemällä on valittavissa yhteensä neljä toimintamallia (Clarke ym. 2004, 70-71). Yleisesti tuotanto- ja teollisuusverkoissa käytössä olevassa kyselymallissa pääasema lähettää pyyntöjä ala-asemalle, joihin ala-asema vastaa. Hiljaisessa mallissa ala-asema taas lähettää tietoja pääasemalle vain, kun tapahtuu muutoksia, joista tulee ilmoittaa pääasemalle. Hiljaisessa mallissa ala-asema kuitenkin usein lähettää pääasemalle tietyin väliajoin viestejä yhteyden toimivuuden varmistamiseksi.

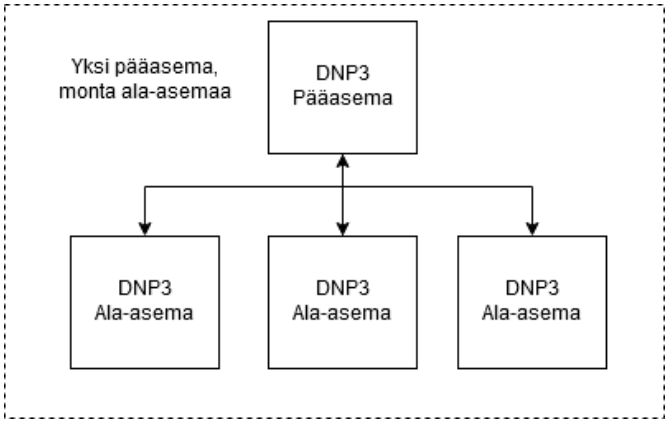
DNP3-protokollassa ala-asema voi siis aloittaa kommunikoimaan pääaseman kanssa, mutta se voi lähettää pääasemalle vain viestejä yhteyden toimivuuden varmistamiseksi. Vain pääasema voi lähettää komentoja tai pyytää tietoa muilta asemilta.

DNP3 tukee useita pääasema ja ala-asema konfiguraatiomalleja. Yksinkertaisin DNP3-topologia on yksi yhteen malli, jossa yksi pääasema on yhteydessä vain yhteen ala-asemaan ja ala-asema on yhteydessä vain yhteen pääasemaan (DNP Users Group 2005, 3). Yksi yhteen malli on nähtävillä kuvassa 2.



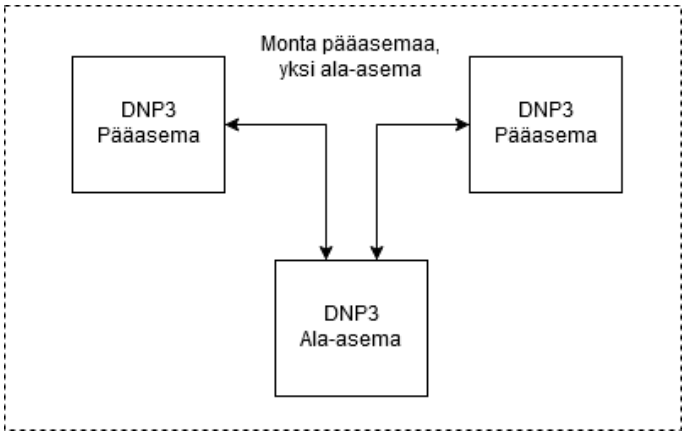
Kuva 2. DNP3-topologia: yksi yhteen.

Yksi pääasema voi ohjata ja lähettää komentoja useille ala-asemille samanaikaisesti. Jokainen ala-asema kommunikoi saman pääaseman kanssa. Mitä enemmän samassa verkossa on laitteita, sen järkevämpi hiljainen toimintamalli on. Hiljaista toimintamallia käyttäessä verkon kuormitus on paljon vähäisempää. (DNP Users Group 2005, 3) Hiljainen malli on esitetty kuvassa 3.



Kuva 3. DNP3-topologia: monta ala-asemaa.

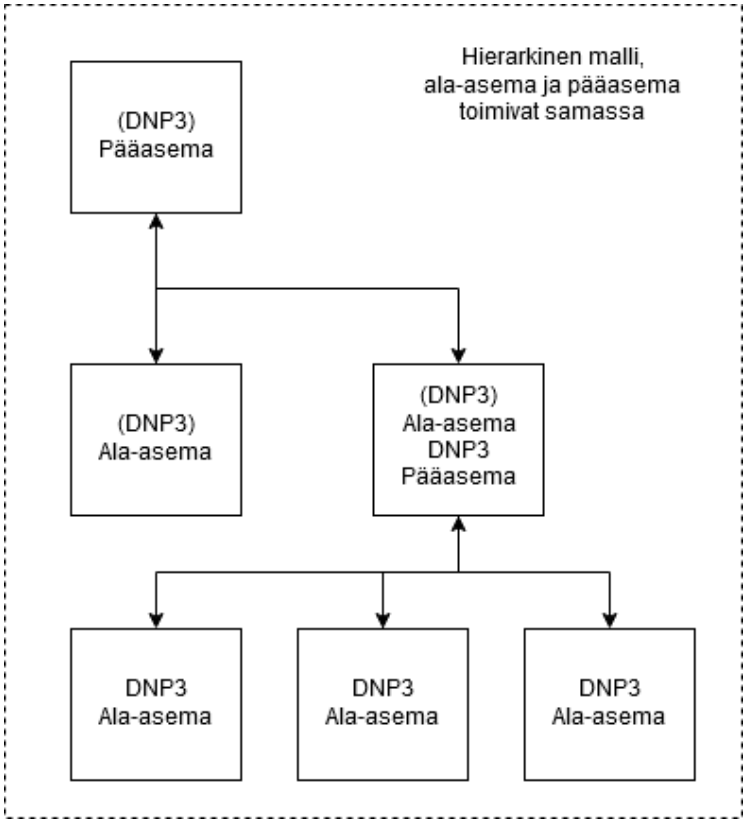
Yksi ala-asema voi myös olla usean pääaseman ohjattavissa. Tällöin ala-asema kommunikoi kahden pääaseman kanssa ja lähettää tietoja niitä pyytäneelle pääasemalle, kuten kuvassa 4 on havainnollistettu. (DNP Users Group 2005, 3)



Kuva 4. DNP3-topologia: monta pääasemaa.

Ala-asema voi myös toimia pääasemana muille ala-asemille järjestelmän eri osassa. Tätä kutsutaan hierarkiseksi malliksi, joka on esitetty kuvassa 5. Hierarkisessa mallissa asema, joka hoitaa niin ala-aseman kuin pääasemankin virkaa saattaa vaihtaa käytettyä protokollaa riippuen kommunikoiko se pääasemana vai ala-asemana (DNP Users Group 2005, 3).

Esimerkiksi jos asema käyttää DNP3-protokollaa vain pääasemana toimiessa, täytyy DNP3-liikenne muuttaa muuhun verkkoon sopivaksi ennen liikenteen lähettämistä ala-asemana eteenpäin seuraavalle pääasemalle, monitorointilaitteeseen tai ohjauskeskukseen.



Kuva 5. DNP3-topologia: hierarkinen malli.

2.2.3 IEC 60870-5

IEC 60870-5 on IEC:n (International Electrotechnical Comission) tuottama kokoelma standardeja, joiden tarkoituksena oli tarjota avoin kommunikaatioprotokolla tuotanto- ja teollisuusjärjestelmien käyttöön. (Clarke ym. 2004, 170)

DNP3 ja IEC 60870-5 ovat molemmat kehitetty samoihin aikoihin ja siksi ne ovat ominaisuuksiltaan samankaltaisia. Kuten DNP3, myös IEC 60870-5 on saanut runsaasti käyttäjiä juuri sen standardoimisen ja avoimuuden takia. IEC 60870-5 on lähinnä sähkölaitosten käytössä, vaikka se soveltuu moneen muuhunkin käyttötarkoitukseen ja liikenne voidaan nykyään ohjata myös TCP/IP-verkon yli. (Clarke ym. 2004, 170)

IEC 60870-5 on yksi kuudesta IEC 60870 -standardin osasta. IEC 60870-5 taas koostuu eri standardeista, jotka määrittelevät protokollan toimintaa tarkemmin. Kaksi tärkeintä standardia ovat IEC 60870-5-101 ja IEC 60870-5-104 (Clarke ym. 2004, 171). Ne määrittelevät yleisesti tuotanto- ja teollisuusverkoissa käytettyjä kommunikaatioprotokollia. IEC 60870-5-101 on alkuperäinen standardi, joka määritteli kommunikaatioprotokollan

kokonaisuudessaan. IEC 60870-5-104 on uudistettu versio, joka määrittelee protokollan käytön TCP/IP-verkon yli (Clarke ym. 2004, 171). IEC 60870-5-104 on nykyään yleisesti käytetty versio, sillä TCP/IP-liikenteen mahdollistaminen on yksinkertaistanut verkkojen rakennetta ja toimintaa.

Järjestelmä, joka käyttää IEC 60870-5 standardeja, ei salli ala-aseman aloittavan kommunikaatiota pääaseman kanssa. Pääaseman tulee aloittaa kaikki kommunikaatio, eli pääaseman tulee lähettää kyselyjä ala-asemille, ennen kuin se olettaa saavansa ala-asemilta mitään tietoa. (Clarke ym. 2004, 172)

Pää- ja ala-asemien välistä kommunikaation aloittamista lukuun ottamatta DNP3 ja IEC 60870-5 ovat toiminnaltaan ja teknisiltä ominaisuuksiltaan hyvinkin samankaltaisia. Tämä johtuu myös paljon tuotanto- ja teollisuusverkkojen vaatimuksista, joihin molemmat protokollat ovat yrittäneet tarjota ratkaisun. (Clarke ym. 2004, 307)

3 PENETRAATIOTESTAUS JA HYÖKKÄYSMENETELMÄT

Penetraatiotestaus on prosessi, jossa määritettyä kohdetta sekä sitä suojaavia tietoturvakontrolleja testataan. Kohde voi olla esimerkiksi sovellus, tietoverkko, prosessi, rakennus tai vaikka yrityksen tai organisaation henkilökunta. Kohteen testaus suoritetaan siihen sopivalla tavalla, käyttämällä soveltuvia työkaluja sekä hyökkäystapoja. Penetraatiotestaus suoritetaan aina testauksen tilaajalta saadun luvan kanssa ja sen aikana löydetyt haavoittuvuudet raportoidaan tilaajalle testauksen lopuksi ennalta sovitulla tavalla, esimerkiksi teknisenä raporttina tai henkilöstön koulutuksena.

Penetraatiotestauksen tavoite on löytää haavoittuvuuksia tai muita tietoturvaongelmia määritetystä kohteesta ennen kuin haitalliset tahot löytävät sekä hyötykäyttävät niitä omiin tarkoituksiinsa. Penetraatiotestauksella voidaan vaikuttaa suoraa kohteen tietoturvan tasoon etsimällä heikkoja kohtia sekä korjaamalla ne asianmukaisesti.

Testaustavat voidaan jakaa helposti kolmeen eri kategoriaan, jotka ovat musta (engl. black box), harmaa (engl. gray box) sekä valkoinen (engl. white box) testausmenetelmä. Mustalaatikkotestauksessa kohde ajatellaan mustana laatikkona eli testaajalla ei ole mitään tietoa kohteesta etukäteen. Valkolaatikko- tai niin sanottu lasilaatikkotestaaminen tarkoittaa että, testaajalla on käytössään tarkkaa tietoa taustajärjestelmistä, ohjelmiston toiminnasta tai mahdollisuus lukea sen lähdekoodia. Harmaalaatikkotestaamisessa yhdistyy hieman molemmat aikaisemmin mainitut tavat. Testaajalla saattaa olla etukäteen jotakin tietoa kohdejärjestelmän toiminnasta tai sen taustajärjestelmistä, mutta vain rajoitetusti. (STF 2019) Harmaalaatikkotestaaminen on hyvin yleinen tapa suorittaa penetraatiotestausta, sillä se ei vaadi koko järjestelmän toiminnan avaamista testaajalle, mutta mahdollistaa tehokkaan tavan testata kohteen tietoturvaa, sillä testauksessa päästään nopeammin liikkeelle.

3.1 Penetraatiotestauksen työvaiheet

Penetraatiotestaus voidaan jakaa seitsemään eri työvaiheeseen. Näissä työvaiheissa tehdään erilaisia toimenpiteitä, jotka mahdollistavat onnistuneen penetraatiotestauksen.

Kaikki työvaiheet ovat tärkeä osa laajempaa testauskokonaisuutta. Testauksen jakaminen eri työvaiheisiin helpottaa sekä selkeyttää testaamisen suorittamista. (PTES 2019)

3.1.1 Testaukseen valmistautuminen

Testauksen ensimmäinen vaihe sisältää usein kokouksen, jossa testauksen osapuolet sopivat testauksen yksityiskohdista. Kokouksessa sovitaan testauksen laajuudesta sekä kestosta. Laajuudella määritetään mitkä kohteet sisältyvät testaukseen ja miten niitä testataan. (PTES 2019) Kohteiden tarkka määrittely auttaa selventämään mitkä asiat kuuluvat penetraatiotestauksen piiriin. On myös tärkeää määrittää aikaraja testauksen suorittamiselle, jotta testauksen syvyys, kattavuus ja sitä kautta hinta voidaan määrittää mahdollisimman tarkasti.

Tilaaja voi vaikuttaa testauksen pääpainotukseen ja määrittää ne asiat, jotka ovat erityisen tärkeitä heille. Molempien osapuolien etu on, että tiedetään mitä testataan, milloin testataan ja miten testataan. Hyvin tehty valmistelu voi säästää paljon aikaa sekä välttää tyytymättömyyttä testaukseen ja on siksi yksi penetraatiotestauksen tärkeimpiä vaiheita.

3.1.2 Tiedonkeruu

Tiedonkeruu tarkoittaa kohdejärjestelmään tutustumista. Tämän vaiheen päämääränä on kerätä kohteesta niin paljon tietoa kuin vain mahdollista. Kerätty tieto osoittautuu usein erittäin hyödylliseksi haavoittuvuuksien löytämisessä sekä etenkin hyväksikäyttämisessä. (PTES 2019) Mitä enemmän tietoa järjestelmän toiminnasta sekä taustajärjestelmistä on onnistuttu keräämään, sen helpompi on testaajan ymmärtää minkälaiset hyökkäystavat toimivat kohdetta vastaan suurimmalla todennäköisyydellä.

Tiedonkeruuseen kuluva aika testauksen alkuvaiheessa riippuu käytettävästä testaustavasta. Esimerkiksi mustalaatikko testauksessa tiedonkeruuseen voi kulua paljonkin aikaa, kun taas lasilaatikko testaamisessa ei niinkään. Lasilaatikko tapaa käyttäen on jo saatu paljon tietoa järjestelmän toiminnasta ja sen taustajärjestelmistä etukäteen, joka nopeuttaa itse testauksen aloittamista. Toisaalta läpikäytävää materiaalia voi olla lasilaatikko testauksessa enemmän, jos mustalaatikko tavalla suoritetussa tiedonkeruuvaiheessa ei onnistuta keräämään kohteesta paljoa tietoa. Tiedonkeruuvaiheeseen tulee

käyttää reilusti aikaa, sillä kunnon pohjatyö varmistaa testauksen sujuvan etenemisen seuraavissa testauksen vaiheissa.

3.1.3 Uhkamallinnus

Uhkamallinnus keskittyy pääasiassa kahteen asiaan, suojattavaan omaisuuteen ja siihen kohdistuviin uhkakuviin. Ennen kuin omaisuuteen kohdistuvat uhat voidaan tunnistaa, tulee ymmärtää kokonaisuudessaan mitä suojattavaa omaisuutta organisaatiolla on. (PTES 2019) Kun tunnistetaan oma omaisuus eli mitä pitää suojata, on helpompi tunnistaa ne uhkakuvat, joilta omaisuutta tulee suojata.

Uhkamallinnus selventää organisaatiolle itselleen, mutta myös penetraatiotestauksen suorittajalle organisaation heikoimpia ja vahvimpia ominaisuuksia sekä minkälaisiin asioihin tulee kiinnittää jatkossa enemmän huomiota (PTES 2019). Uhkamallinnuksen avulla voidaan siis rakentaa kokonaiskuva organisaatiota koskevista uhista ja niiden vaikutuksista kohdeorganisaation toiminnan jatkuvuuteen.

Kokonaiskuvaa voidaan rakentaa jaottelemalla erilleen liiketoiminnan kannalta tärkeimmät omaisuudet sekä prosessit. Uhkakuvat sen sijaan voidaan hahmottaa selvemmin jakamalla ne uhkayhteisöihin eli hyökkääjiin sekä hyökkääjien kyvykkyyteen suorittaa hyökkäyksiä. (PTES 2019) Kun kokonaiskuva on luotu, voidaan identifioida ja kategorisoida organisaatiota koskevat uhat.

Omaisuuden, prosessien sekä uhkayhteisöjen ja niiden kyvykkyyden identifioinnin jälkeen hyökkääjien vaikutusta organisaation omaisuuteen sekä prosesseihin on mahdollista mallintaa tarkemmin. Mallinnuksella pyritään selkeyttämään kokonaiskuvaa sekä löytämään tärkeimpiä asioita, joihin tulee kiinnittää erityistä huomiota. (PTES 2019)

3.1.4 Haavoittuvuusanalyysi

Haavoittuvuusanalyysissa keskitytään löytämään haavoittuvuuksia kohdejärjestelmästä. Löydetyt haavoittuvuudet voivat vaihdella palvelun toimintatapoja paljastavista virheilmoituksista koko palvelun haltuunoton mahdollistaviin haavoittuvuuksiin. Kattavan testaustuloksen saamiseksi on tärkeää käydä kohde tarkasti läpi ja testata kaikki sen sisältämät ominaisuudet. (PTES 2019) Haavoittuvuusanalyysissä tulee myös noudattaa tilaajan kanssa sovittuja rajoja ja painottaa testaamista sitä vaativille osa-alueille.

Haavoittuvuusanalyysissa voidaan käyttää apuna erilaisia työkaluja, jotka auttavat testaajaa havaitsemaan mahdollisia haavoittuvuuksia. Testaamista tulisi kuitenkin suorittaa lähtökohtaisesti manuaalisesti parhaan tuloksen saamiseksi, joitakin testauksen osia voidaan myös automatisoida testauksen sujuvoittamiseksi. Automaattiset työkalut eivät kuitenkaan välttämättä löydä kaikkea, mitä kokenut testaaja kykenee havaitsemaan manuaalisella testaamisella.

3.1.5 Haavoittuvuuksien hyödyntäminen

Haavoittuvuuksien hyödyntämisvaiheessa käytetään hyväksi haavoittuvuusanalyysissa löydettyjä haavoittuvuuksia. Vaiheen päätarkoituksena on suorittaa onnistunut hyökkäys kohdetta vastaan käyttämällä löydettyjä haavoittuvuuksia. (PTES 2019) Jos aikaisemmat vaiheet on suoritettu hyvin, haavoittuvuuden hyödyntäminen helpottuu jonkin verran.

Onnistunut hyökkäys voi tarkoittaa luvattoman pääsyn saamista järjestelmään, salatun tiedon paljastamista järjestelmästä tai jonkin muun hyökkäyksen toteuttamista. Tarkka onnistuneen hyökkäyksen määritelmä riippuu kohteesta ja tilaajan ilmoittamista vaatimuksista testaukselle.

3.1.6 Haavoittuvuuksien jatkohyödyntäminen

Haavoittuvuuksien löytämisen ja niiden onnistuneen hyväksikäytön jälkeen, voidaan siirtyä haavoittuvuuksien hyödyntämiseen osana jatkohyökkäyksiä. Tällaisten hyökkäyksien tarkoitus on usein saada pääsy muihin järjestelmiin tai onnistua korottamaan omia käyttöoikeuksia järjestelmässä. Jatkohyödyntämisessä pyritään löytämään reitti syvemmälle kohdeorganisaatioon järjestelmiin. (PTES 2019)

Haavoittuvuuksien jatkohyödyntämisessä on tärkeää noudattaa sovittuja testaussääntöjä, sillä tuotantoympäristöön tunkeutuessa vastaan saattaa tulla hyvinkin arkaluontoista tietoa (PTES 2019). Usein löydetyt haavoittuvuudet ja keinot päästä palvelimelle tai sisäverkkoon sisään ovat jo hyvin arkaluontoisia itsessään. Haavoittuvuuksien jatkohyödyntäminen ei aina ole osana testausta ollenkaan, vaan testauksessa keskitytään haavoittuvuuksien löytämiseen sekä niiden vaikutuksen esittämiseen testauksen tilaajalle.

3.1.7 Raportointi

Penetraatiotestauksen viimeinen vaihe on raportointi, jonka tarkoituksena on testauksen aikana tehtyjen havaintojen tuominen testauksen tilaajan tietoon. Raportointi voidaan suorittaa eri tavoilla, riippuen mitä on testattu. Esimerkiksi teknisen järjestelmän testaustuloksista voidaan raportoida teknisellä raportilla, joka selvittää miten haavoittuvuutta hyödynnettiin ja mikä sen vaikutus kohdejärjestelmään on. Jos taas on testattu organisaation henkilökuntaa esimerkiksi tietojenkalastelukampanjalla, on luultavasti mielekkäämpää raportoida tuloksista henkilöstön koulutuksen muodossa.

Oli raportin toimitustapa mikä hyvänsä, se on erittäin tärkeä osa koko testausprosessia. Testauksesta tulisi aina toimittaa jonkinlainen raportti tai tiedoksianto tehdyistä havainnoista. Ilman testauksen pohjalta luotua raporttia testauksen tulokset jäävät helposti liian vähälle huomiolle ja tarvittavat korjaukset jäävät tekemättä. Jos tehdyt havainnot sisältävät kriittisiä haavoittuvuuksia ja niitä ei korjata huonon tai olemattoman raportoinnin vuoksi, voi siitä myöhemmin seurata organisaatiolle isojakin ongelmia. Haitallisen tahon löytäessä ja hyödyntäessä korjaamatonta haavoittuvuutta se voi haavoittuvuudesta riippuen aiheuttaa suurta haittaa organisaation toiminannan jatkuvuudelle.

3.2 Hyökkääminen tuotanto- ja teollisuusjärjestelmiä vastaan

Tuotanto- ja teollisuusverkkojen haavoittuvuudet voidaan jakaa kolmeen kategoriaan, käyttäjien virheisiin, konfiguraatiovirheisiin sekä tietoturvan kannalta puutteettomaan suunnitteluun. Tuotanto- ja teollisuusverkot koostuvat erilaisista protokollista ja verkkolaitteista, joiden kaikkien tietoturvalliseen toimintaan tulee kiinnittää huomiota. (Weed 2017, 4)

Laajemmat kohdistetut hyökkäykset tuotanto- ja teollisuusjärjestelmiä kohtaan ovat usein tarkoin harkittuja, sillä niihin kohdistetun hyökkäyksen suorittaminen vaatii paljon resursseja. Perehtyminen kohteeseen eli penetraatiotestauksen tiedonkeruuvaihe vie vaatii paljon aikaa, sillä usein koko hyökkäyksen onnistuminen perustuu kohteesta kerätyn tiedon pohjalta suunniteltuun tarkkaan hyökkäykseen.

Laajoja hyökkäyksiä kykenevät suorittamaan valtiolliset toimijat, rikollisjärjestöt, kilpailevat yritykset, terroristijärjestöt tai muut aatteellisesti motivoituneet ryhmittymät (Weed

2017, 7–8). Tällaisilla ryhmillä on usein aikaa, osaamista sekä rahaa kohdistettujen hyökkäyksien suorittamiseen.

Hyökkääjien motivaationa on usein laitoksen tai sen omistavan yrityksen suunnitelmien, patenttien tai muiden immateriaalisen omaisuuden varastaminen tai haitan aiheuttaminen kohteen liiketoiminnan jatkuvuudelle (Weed 2017, 7). Muita syitä hyökkäyksille voivat olla haitan aiheuttaminen tuotanto- ja teollisuusverkkojen prosesseille kilpailuedun saavuttamiseksi, oman aatteen tai kyseisen organisaation toiminnan vastustamisen esilletuominen aiheuttamalla kohteen toiminnalle haittaa.

Nykyään lisääntyneet kiristysohjelma -hyökkäykset ovat yleistyneet huomattavasti. Kiristysohjelmat lukitsevat saastuneen laitteen tiedostot ja estävät siten sen käytön kokonaan. Tiedostot voi saada takaisin maksamalla lunnaat, joskin ei ole mitään takuita, että tiedostot saa oikeasti takaisin. Kiristysohjelmat ovat tehokkaita työkaluja yrityksiä, sairaaloita ja muita suuria organisaatioita vastaan, sillä niillä on käytössä paljon verkkoon liitettyjä laitteita. Mitä kriittisempi kohteen toimiala on, sitä varmemmin kohde taipuu maksamaan lunnaat, jotta normaalia toimintaa voidaan jatkaa keskeytyksettä. Tuotanto- ja teollisuusjärjestelmät ovat mielenkiintoisia kohteita kiristysohjelmien levittäjille, sillä ne ovat usein erittäin kriittisiä laitoksia, joiden toiminnan jatkuvuus on taattava.

Niin sanotut opportunistiset hyökkääjät sattuvat löytämään järjestelmästä haavoittuvuuden ilman sen suurempaa motivaatioita hyökätä juuri kyseistä kohdetta vastaan. Opportunistinen hyökkääjä saattaa käyttää löytämäänsä haavoittuvuutta hyödyttääkseen itseään.

3.3 Aikaisempia hyökkäyksiä tuotanto- ja teollisuusjärjestelmiin

Tuotanto- ja teollisuusverkkoja kohtaan on hyökätty aikaisemmin, mutta kaikkia epäiltyjä hyökkäyksiä ei olla voitu varmistaa. Sillä tuotanto- ja teollisuusjärjestelmiin hyökkäävät tahot ovat saattavat usein olla valtiollisen toimijan tukemia, voi hyökkäyksen tutkiminen ja virallinen varmistaminen aiheuttaa diplomaattisia selkkauksia. Lisäksi kohdistettuja hyökkäyksiä suorittavat tahot ovat usein erittäin taitavia, heillä on paljon resursseja käytössä ja siten heidän suorittamien hyökkäyksien tutkiminen voi olla hyvin vaikeaa.

Vaikka hyökkäyksiä ei voida aina varmistaa on silti mahdollista tehdä johtopäätöksiä tarkastelemalla minkälaisia motiiveja eri tahoilla saattaa olla suorittaa kyseinen hyökkäys.

Maailmanpoliittiset tilanteet ja eri valtioiden intressit selittävät usein paljon erilaisten hyökkääjätahojen toimintaan.

3.3.1 Stuxnet

Stuxnet on tarkasti tuotanto- ja teollisuusjärjestelmiä vastaan suunniteltu haittaohjelma. Sen kehittivät Yhdysvallat yhteistyössä Israelin kanssa. Stuxnetin tarkoitus oli häiritä Iranin uraaninrikastamon toimintaa ja siten hidastaa Iranin ydinohjelmaa (Ars Technica 2012). Ydinohjelman häiritseminen hidasti suoraa Iranin ydinaseiden kehittämistä ja oli siksi Yhdysvaltojen sekä Israelin hyökkäyksen kohteena.

Iranin uraaninrikastamosta ei ollut yhteyttä internettiin laitoksen arkaluontoisuuden vuoksi. Stuxnet- haittaohjelma tulikin saada saastuttamaan laitoksen laitteita muuta reittiä. Stuxnet onnistuttiin saamaan uraaninrikastamon sisälle muistitikun avulla, jolloin se pääsi leviämään myös tuotantoympäristöön. Stuxnet oli todella tarkasti kohdennettu Iranin käyttämiä laitteita ja protokollia kohtaan ja se hyödynsi toiminnassaan useita nollapäivähaavoittuvuuksia. (Ars Technica 2012) Useiden nollapäivähaavoittuvuuksien hyödyntäminen on selvä merkki, että kyseessä on hyvillä resursseilla tuettu hyökkäyskampanja.

Stuxnet oli suunniteltu aktivoitumaan vain aika ajoin, jolloin sitä oli vaikeampi havaita. Kun Stuxnet aktivoitui, se häiritsi tuotantoprosesseja rikkomalla tuotantolaitteita muokkaamalla niille välitettyjä komentoja. Samalla monitorointilaitteille lähetettiin tietoa, että tuotantoympäristössä oli kaikki niin kuin kuuluikin, vaikka laitteistoa todellisuudessa hajosi jatkuvasti kovempaan tahtiin kuin olisi kuulunut. (Ars Technica 2012)

Ajan myötä Stuxnet kehitettiin leviämään voimakkaammin, jotta uraaninrikastamon toimintaa voitiin häiritä voimakkaammin. Voimakas leviäminen kuitenkin aiheutti muidenkin ympäristöjen saastumisen ja lopulta Stuxnetin hallinta menetettiin täysin vuonna 2010 (Ars Technica 2012).

3.3.2 Black Energy

Toisin kuin Stuxnet, Black Energy ei ollut suoraan tuotanto- ja teollisuusjärjestelmiä vastaan kohdistettu haittaohjelma. Sen sijaan sitä hyödynnettiin hyökkäyksessä, joka oli tarkasti kohdistettu tuotantoympäristöön.

Joulukuussa 2015, noin 1,4 miljoonaa ukrainalaista jäi ilman sähköä muutamaksi tunniksi kyberhyökkäyksen vuoksi. Ukrainan sähkönjakelulaitoksia vastaan oli kohdistettu useita hyökkäyksiä samaan aikaan, ja ennen sähkönjakelulaitoksia vastaan tehtyjä hyökkäyksiä, oli Ukrainan kriittinen infrastruktuuri ollut useiden muidenkin kyberhyökkäysten kohteena. Tekijästä tai hyökkäyksien yhteyksistä toisiinsa ei ole varmuutta. (We Live Security 2016)

Black Energy on tunnettu haittaohjelma, jota on käytetty osana useita erilaisia hyökkäyksiä vuosien varrella. Sitä oli käytetty myös muissa Ukrainaan kohdistuneissa hyökkäyksissä aikaisemmin samana vuonna.

Sähkönjakelulaitoksiin kohdistuneet hyökkäykset olivat hyvin yksinkertaisia ja niissä hyödynnettiin sähköpostissa lähetettyjä Microsoft Excel -tiedostoja. Viesti näytti, että se tuli Ukrainan parlamentilta, vaikka todellisuudessa sen olivat lähettäneet hyökkääjät. Excelissä luki, että makrot tulisi ottaa käyttöön tai tiedosto ei toimisi oikein. Makrot sisälsivät haitallista koodia, joka saastutti tiedoston avaajan Black Energy- haittaohjelmalla. (We Live Security 2016)

Aikaisemmat Ukrainasta löydetyt Black Energy- haittaohjelmat ovat sisältäneet vain ominaisuuksia, jolla voidaan tuhota tiedostoja. Sähkölaitoksista löydetyt haittaohjelmat sisälsivät kuitenkin erityisesti tuotanto- ja teollisuusverkkoja vastaan kohdistettuja ominaisuuksia. Sähkölaitoksista löydetyt Black Energyn versiot yrittivät lopettaa tietyn prosessin. Prosessi kuului yleisesti tuotanto- ja teollisuusjärjestelmissä käytössä olevalle ohjelmalle. Jos prosessi onnistuttiin lopettamaan onnistuneesti, yritti haittaohjelma myös kirjoittaa kyseisen prosessin suoritustiedoston päälle roskadataa. (We Live Security 2016)

Hyökkäys oli siis selvästi kohdistettu tuotanto- ja teollisuusjärjestelmiä vastaan, vaikka se ei suoranaisesti hyödyntänyt tuotanto- ja teollisuusverkoissa toimivaa haittaohjelmaa.

4 TUOTANTO- JA TEOLLISUUSVERKON TESTAUS

4.1 Testauksen tavoitteet

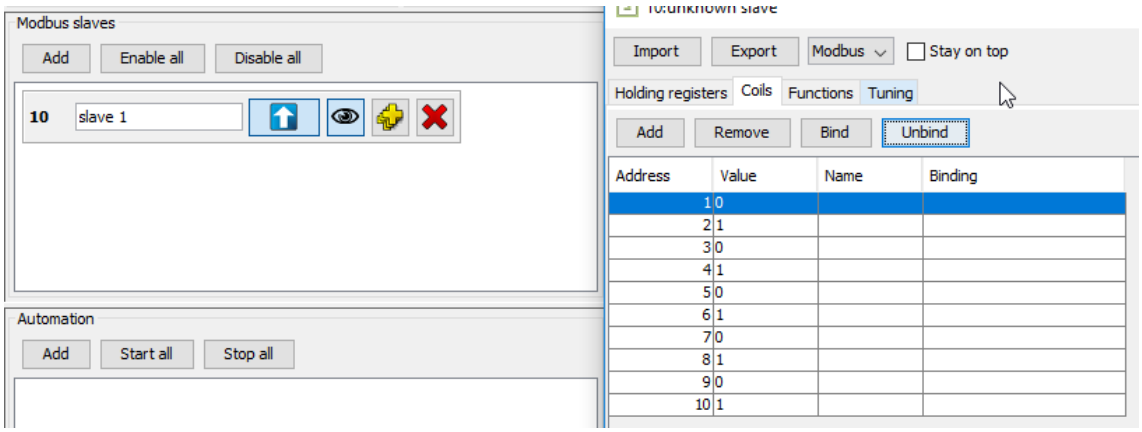
Virtuaaliympäristössä suoritetun tuotanto- ja teollisuusverkon testauksen tavoitteena oli onnistua uudelleentoistamaan järjestelmien ja protokollien tunnettuja haavoittuvuuksia sekä yleisesti tarkastella verkon toimintaa tietoturvan näkökulmasta. Testauksen päätavoite oli simuloida hyökkääjää, jonka tarkoituksena on vaikuttaa tuotantoprosessiin ja siten aiheuttaa kohdeorganisaation toiminnalle haittaa.

Erityistä huomiota kiinnitettiin prosessien häirintään eli hyökkäyksiin, joilla voidaan muunnella verkkolaitteiden lähettämää ja vastaanottamaa dataa, ja siten vaikuttaa järjestelmän prosesseihin. Näillä hyökkäystavoilla voidaan aiheuttaa tuotanto- ja teollisuusverkkojen toiminnalle suurta haittaa.

4.2 Testausympäristö

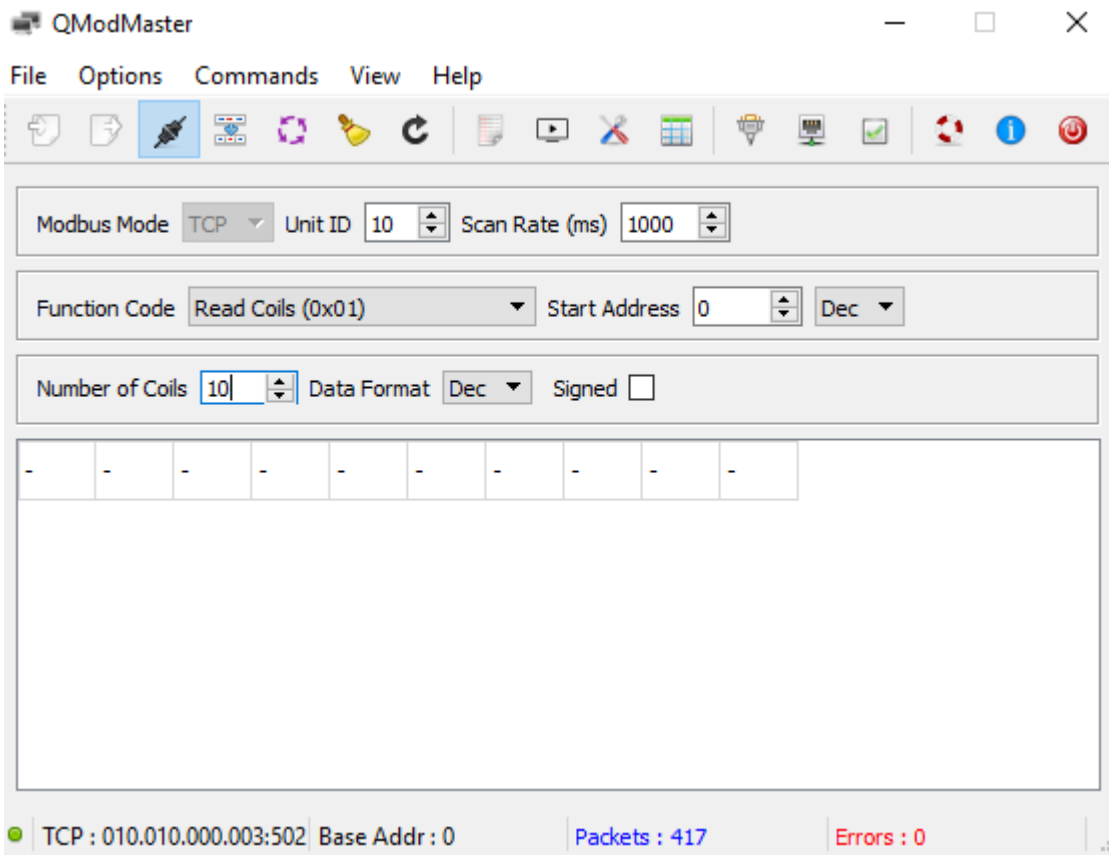
Testausympäristön toteuttamisessa käytettiin VirtualBox -virtualisointiohjelmaa, jonka avulla asennettiin kaksi virtuaalikonetta Windows 10 -käyttöjärjestelmällä sekä yksi Kali Linux. Kali Linux toimi hyökkääjän koneena verkossa, jolloin virtuaaliverkkoon ei tarvinnut rakentaa hyökkääjän liikenteelle erillistä pääsyä.

Ala-asemana toimivalle Windows 10 -koneelle asennettiin ModbusPal 1.6b, jolla simuloitiin ala-asemaa ja sen modbus-liikennettä. ModbusPalia käyttäen luotiin laite, jonka yksikkö ID oli 10. Laitteen lähettämät arvot simuloivat kentältä kerättyä tietoa ja arvot olivat vuorotellen 0 ja 1. Kuvassa 6 on ModbusPaliin määritetty edellä mainitun mukainen konfiguraatio.



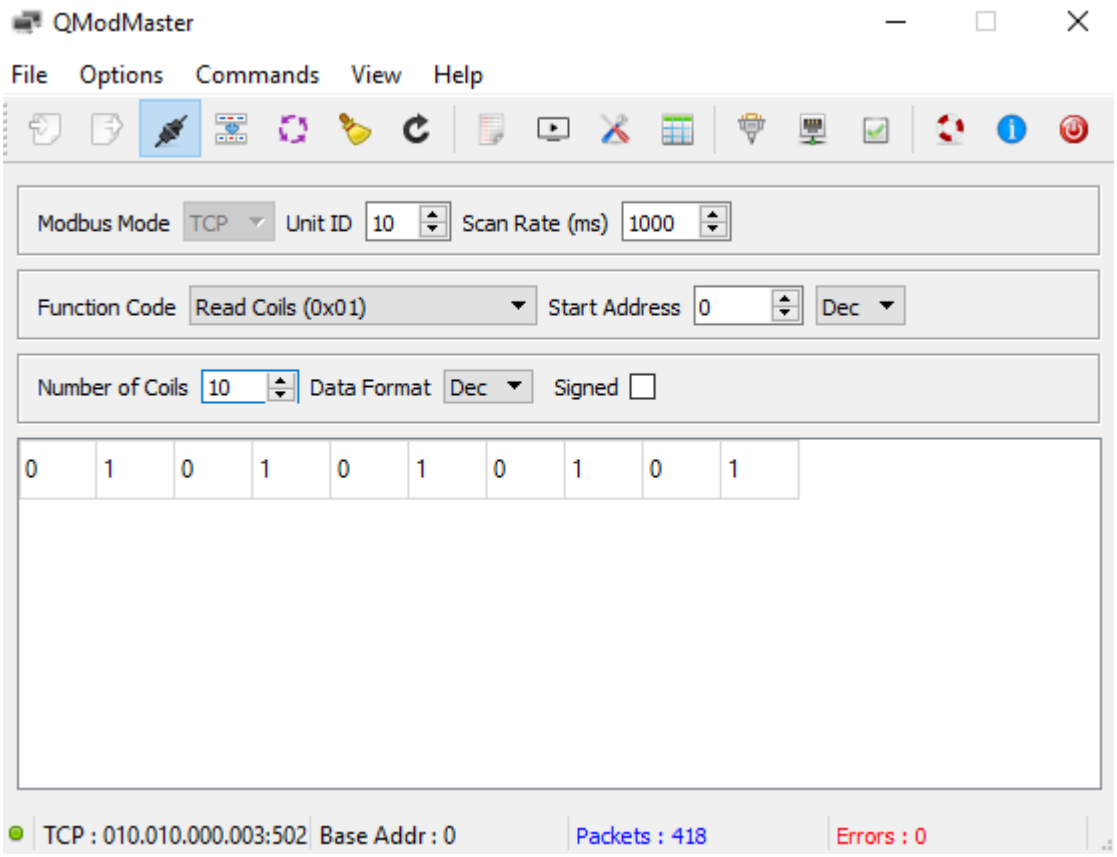
Kuva 6. Ala-aseman konfiguraatio.

Pääasemana toimivalle Windows 10 -koneelle asennettiin QModMaster, johon määritettiin ala-aseman IP-osoite sekä käytetty portti. Näiden lisäksi piti määrittää yksikön numero ja pyydettävien tietueiden määrä, kuten kuvassa 7 näkyy.



Kuva 7. Pääaseman konfiguraatio.

Kun tarvittavat tiedot oli saatu määritettyä, voitiin pääasemalta tehdä pyyntöjä ala-asemalle, jolloin arvot siirtyivät ala-asemalta pääasemalle, kuvan 8 mukaisesti. Pääaseman vastaanottamien arvojen perusteella olisi voitu suorittaa toimenpiteitä tai lähettää ne eteenpäin monitoroitavaksi.



Kuva 8. Pääaseman ja ala-aseman välinen tiedonsiirto.

Tieto siirtyi ala-asemalta pääasemalle ongelmitta eli testiympäristö toimi kuten pitikin. Huomioitavaa on, että kerätty tieto on aina sama, sillä oikeaa tietoa ei testiympäristössä voitu kerätä. Pääaseman ala-asemalta saamaa tietoa ei myöskään lähetetty eteenpäin tai sen pohjalta ei suoritettu minkäänlaisia toimenpiteitä, sillä se ei ollut testauksen kannalta oleellista.

4.3 Hyökkäyssimulaatio

Tuotantoympäristön testauksen ajatuksena oli simuloida oikeaa hyökkääjää, jonka tavoitteena oli häiritä kohdeorganisaation tuotantoprosesseja. Ensimmäinen testauksen hyökkäysosa oli penetraatiotestausmallin mukaisesti tiedonkeruu verkkoympäristöstä.

Testaus alkoi ajatuksesta, että hyökkääjä on jo päässyt tunkeutumaan verkkoympäristöön.

Tiedonkeruu aloitettiin skannaamalla koko tuotantoverkko Nmap-työkalulla. Verkosta löytyi virtuaalireitittimen lisäksi kaksi laitetta, jotka porttiskannattiin tarkemmin lisätiedon keräämiseksi. Toisesta laitteesta löytyi avoin portti 502, joka on yleisesti modbus-liikenteessä käytetty portti, joten se viittaa heti vahvasti tuotantoverkkolaitteeseen.

Tiedonkeruun avulla voitiin päätellä, että kyseessä todellakin oli tuotantoympäristö, jossa mitä todennäköisimmin oli Modbus-liikennettä. Näillä alkutiedoilla voitiin siirtyä penetraatiotestauksen uhkamallinnusvaiheeseen. Uhkamallinnuksessa tarkoituksena oli tunnistaa mahdollisia heikkoja kohtia ja järjestelmän suurimpia uhkaskenaarioita. Tässä tapauksessa tarkoituksena oli häiritä prosessia, joten liikenteen muokkaaminen olisi toimiva hyökkäysvektori.

Haavoittuvuusanalyysivaiheessa aloitettiin haavoittuvuuksien etsiminen. Kali Linuxin mukana tulevan Ettercap-ohjelman avulla suoritettiin ensin ARP-väärennös. Tällä hyökkäyksellä koneiden välinen liikenne saatiin kulkemaan hyökkääjän koneen kautta, jolloin sitä voitiin tarkastella tarkemmin ja varmentaa tieto laitteiden välisestä Modbus-liikenteestä.

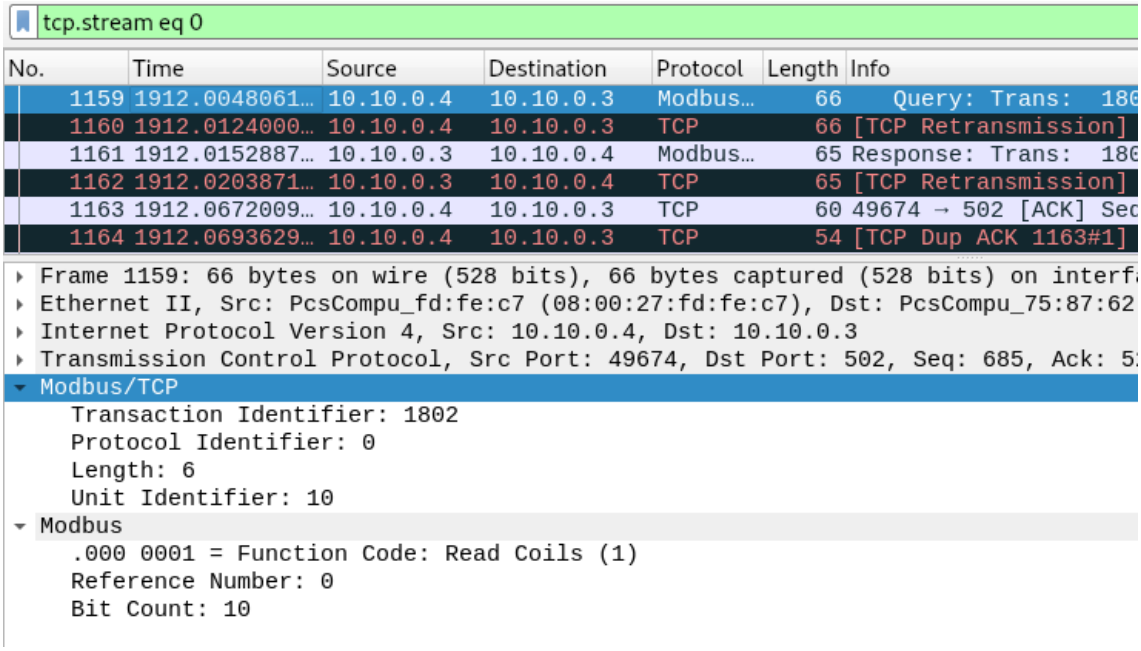
Ettercap-ohjelma tarvitsi ensin laitteiden osoitteet. Nämä tiedot oli kerätty Nmap-skannauksen tuloksena, mutta Ettercap osasi löytää ne myös itse. Jos verkossa olisi ollut enemmän laitteita, olisi tiedonkeruuvaihe noussut suurempaan rooliin. Kun oikeat kohteet oli määritetty Ettercapiin, voitiin aloittaa ARP-viestien väärentäminen osana penetraatiotestauksen haavoittuvuuksien hyödyntämisvaihetta. Kuvassa 9 on kuvattuna ARP-väärennöksen suoritus Ettercapilla.

```
2 hosts added to the hosts list...
Resolving 2 hostnames...
Host 10.10.0.3 added to TARGET1
Host 10.10.0.4 added to TARGET2

ARP poisoning victims:

GROUP 1 : 10.10.0.3 08:00:27:3F:6E:E5

GROUP 2 : 10.10.0.4 08:00:27:FD:FE:C7
```

Kuva 9. ARP-väärennös Ettercapilla.

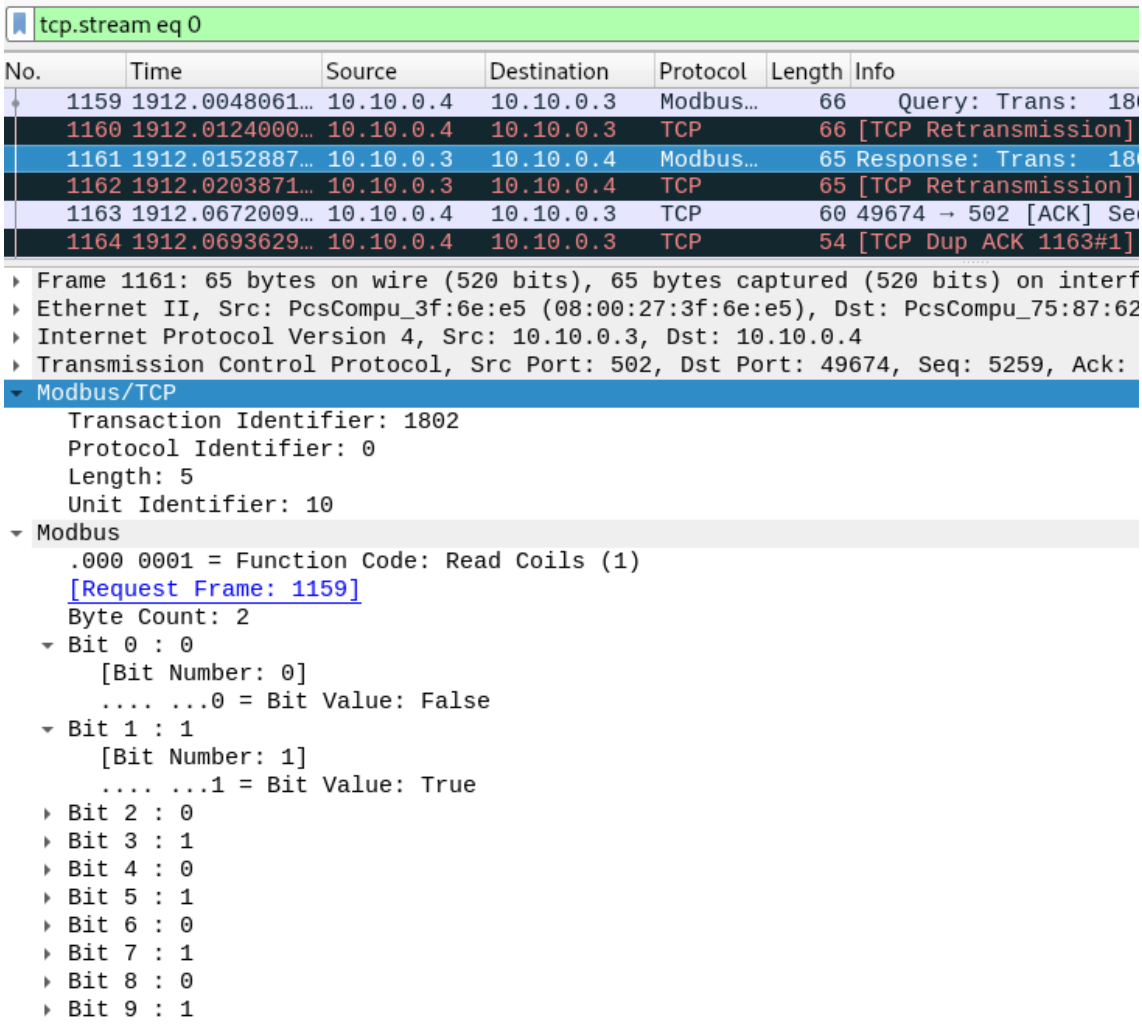
Ettercapin avulla suoritettu ARP-väärennös mahdollisti kohdelaitteiden välisen liikenteen tarkasteleminen Wireshark-ohjelmalla. Wiresharkissa alkoikin heti näkyä Modbus kyselyitä sekä vastauksia niihin. Liikenteestä nähtiin myös, että paketit kulkivat ala-asemalla portin 502 kautta.

Kuvan 10 mukaisista Modbus -kyselyistä selvisi yksikön ID, pyydettyjen tietueiden määrä sekä pyydetty toiminto, sillä liikenne oli täysin salaamatonta. Liikenteen salaamattomuus oli ensimmäinen haavoittuvuus.



Kuva 10. Modbus -kysely.

Modbus -vastauksesta sen sijaan selvisi enemmän, sillä se sisälsi ala-asemalta lähetetyn vastauksen pääaseman kyselyyn. Kuvan 11 sisältämästä Modbus -vastauksesta näkyy yksikön ID sekä jokaisen pyydetyn tietueen arvo, jotka ovat vuorotellen 0 ja 1, kuten ne olivat ala-aseman ModbusPal ohjelmaan määritelty.



Kuva 11. Modbus -vastaus.

Hyödyntämällä ARP-väärennöstä voitiin ala-aseman sekä pääaseman välistä Modbus-liikennettä lukea. Tässä tapauksessa liikenne ei sisällä arkaluontoista tietoa, mutta salaamaton liikenne altistaa muille hyökkäyksille.

Salaamatonta eli selkokielistä liikennettä voidaan myös muokata, sillä laitteet eivät käytä tiedonvälityksessä minkäänlaista autentikointia. Autentikoinnin puute tarkoittaa, että laitteet eivät varmista tiedon lähdettä, jolloin tietoa voidaan muokata mielivaltaisesti. Salaamaton liikenne on haavoittuvuus protokollassa, jota voitiin hyödyntää lukemalla liikennettä. Haavoittuvuutta voidaan jatkohyödyntää suorittamalla salauksen puutteen mahdollistamia muita hyökkäyksiä.

Liikennettä voitiin muokata helposti käyttämällä siihen kehitettyä MetaSploit-moduulia modbusclient. Moduulin onnistunut suorittaminen muutti valittua arvoa ala-asemalla, josta se siirtyi pääasemalle kyselysyklin osuessa kohdalle.

MetaSploit ohjelman käynnistyksen jälkeen valittiin käytettäväksi modbusclient-moduuli ja hyökkäykseen vaaditut asetukset säädettiin oikein.

Kuvassa 12 näkyy, kuinka asetuksissa määritettiin kirjoitettava arvo (data 0), ylikirjoitettavan arvon osoite (data_address 1), kohteen IP-osoite (rhosts 10.10.0.3) sekä yksikön ID (unit_number 10). Asetuksiin vaaditut tiedot saatiin kerättyä tarkastelemalla salaamatonta liikennettä Wiresharkilla.

```
msf5 auxiliary(scanner/scada/modbusclient) > set data 0
data => 0
msf5 auxiliary(scanner/scada/modbusclient) > set data_address 1
data_address => 1
msf5 auxiliary(scanner/scada/modbusclient) > set rhosts 10.10.0.3
rhosts => 10.10.0.3
msf5 auxiliary(scanner/scada/modbusclient) > set unit_number 10
unit_number => 10
msf5 auxiliary(scanner/scada/modbusclient) >
```

Kuva 12. Modbusclient asetukset.

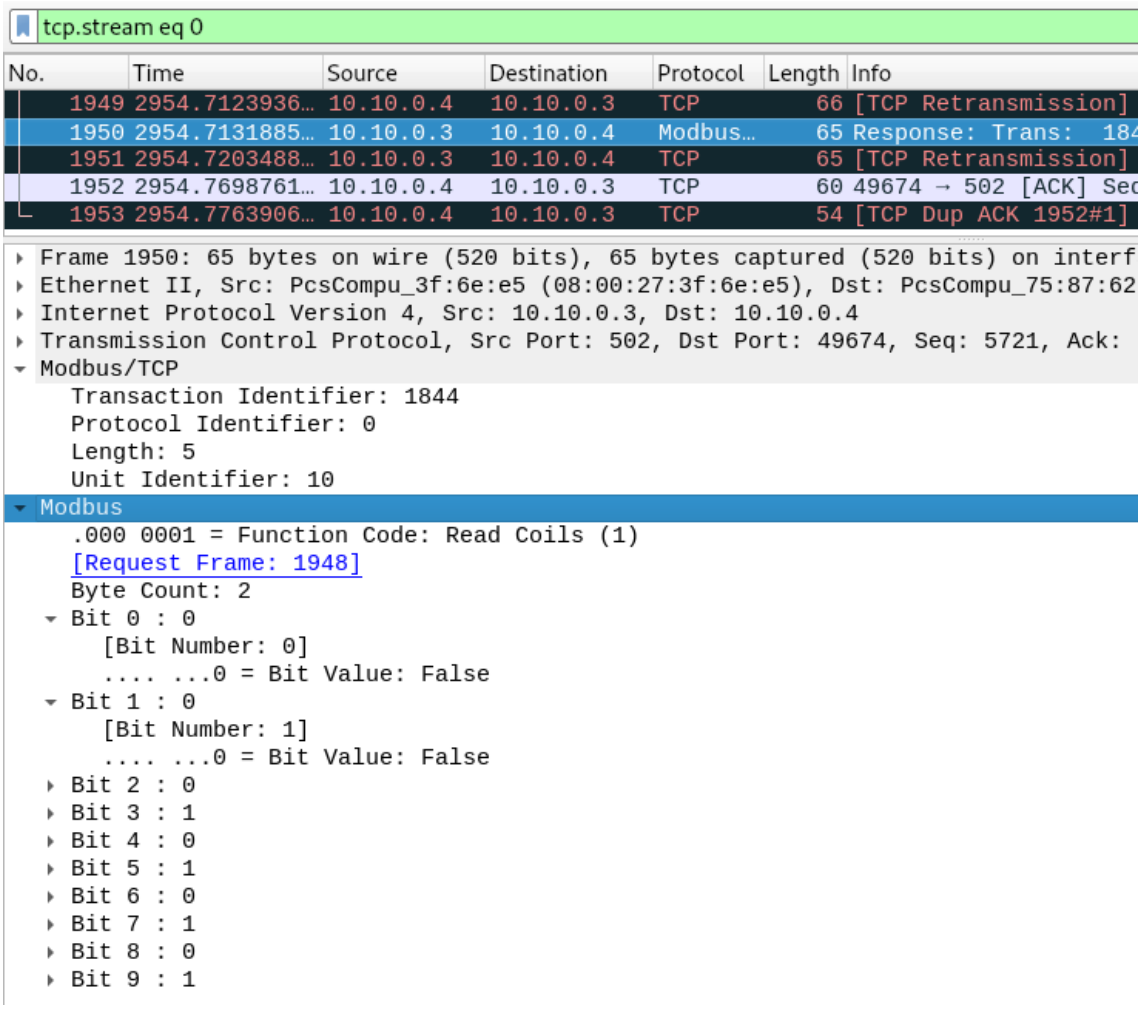
Kun kaikki asetukset oli asetettu, voitiin hyökkäys suorittaa. Moduuli ilmoitti kuvan 13 mukaisesti, kun hyökkäys on suoritettu onnistuneesti ja arvo 0 kirjoitettiin osoitteeseen 1.

```
msf5 auxiliary(scanner/scada/modbusclient) > run

[*] 10.10.0.3:502 - Sending WRITE COIL...
[+] 10.10.0.3:502 - Value 0 successfully written at coil address 1
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/scada/modbusclient) >
```

Kuva 13. Modbusclient hyökkäys.

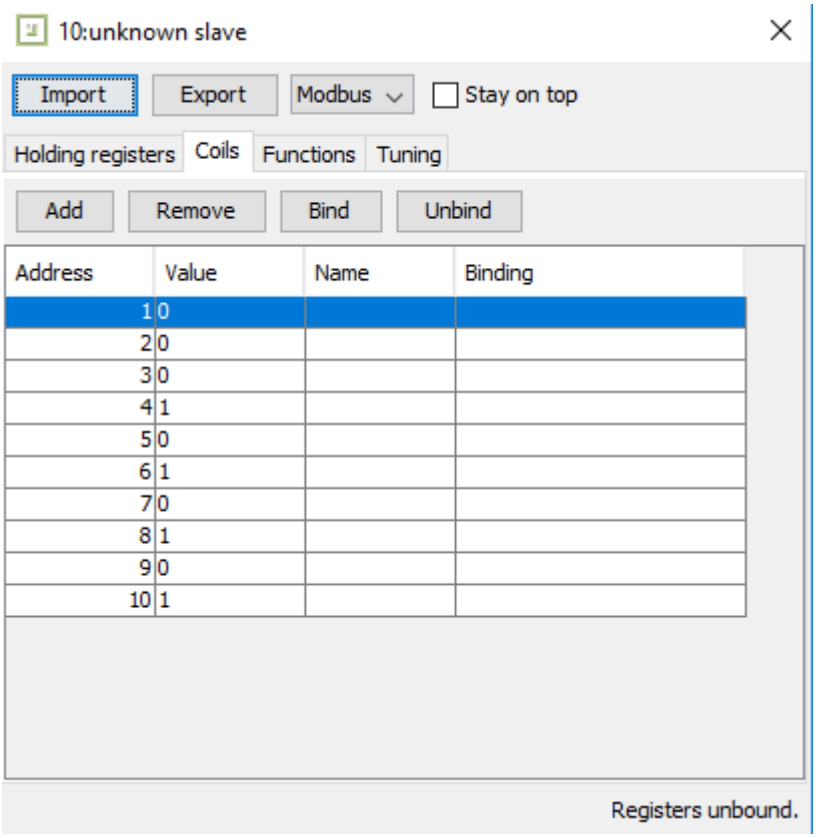
Hyökkäys muutti arvoa ala-asemalla, josta se siirtyi pääasemalle modbus kyselyn tuloksena. ARP-väärennöstä ei moduulin suorittamiseen tarvittu, mutta sen avulla voitiin muutettuja arvoja seurata Wiresharkin kautta.

Kuvassa 14 näkyy muutettu arvo osoitteessa 1. Arvo oli aikaisemmin 1, mutta hyökkäyksen onnistuminen voitiin todentaa, sillä ala-asema lähetti pääasemalle hyökkäyksen takia arvon 0.



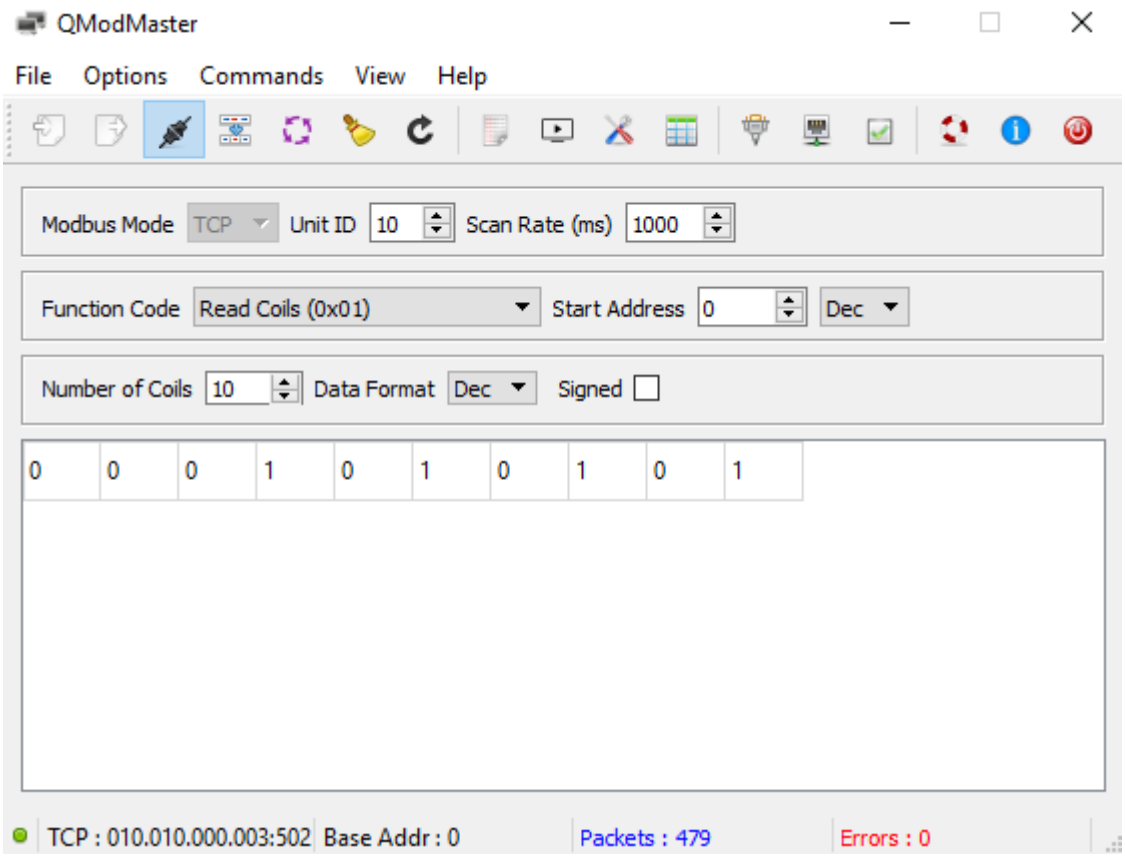
Kuva 14. Modbusclient hyökkäys Wiresharkissa.

Onnistuneen hyökkäyksen uudelleentarkastamiseksi ala-aseman arvot luettiin ModbusPal ohjelman kautta. Kuvassa 15 näkyy kuinka osoitteen 1 arvoksi on muuttunut 0. Arvot eivät enää ole vuorotellen 0 ja 1, vaan aluksi on kolme samaa arvoa.



Kuva 15. Modbusclient hyökkäys ala-asemalla.

Kuvasta 16 huomataan, että hyökkäys näkyy pääasemalla samalla tavoin kuin ala-asemalla. Ala-asemalta saadut arvot eivät ole vuorotellen 0 ja 1. Arvot alkavat kolmella samalla arvolla, jonka jälkeen ne ovat vuorottain 0 tai 1. Hyökkäys muokkasi tuotantoympäristössä kulkevaa liikennettä onnistuneesti, ja tuotantoprosessiin pystyttiin vaikuttamaan protokollan tietoturvapuutteiden vuoksi.



Kuva 16. Modbusclient hyökkäys pääasemalla.

5 LOGIIKKAKONTROLLERIHUNAJAPURKKI

Hunajapurkki (engl. honeypot) on järjestelmä, jonka tarkoituksena on hämätä hyökkääjää luulemaan sitä oikeaksi järjestelmäksi ja kohdistamaan hyökkäyksensä sitä kohtaan. Hunajapurkissa ei kuitenkaan ole tuotantodataa, vaan se ottaa lokeihin talteen kaikki siihen otetut yhteydet (Norton 2019). Hunajapurkkeja käytetään tiedon keräämisen hyökkäyskampanjoista ja niitä käytetään esimerkiksi yrityksissä hyökkäyksien ja tunkeutujien tunnistamiseen. Myös tietoturvayritykset tunnetusti käyttävät hunajapurkkeja tiedon keräämiseen uusista haittaohjelmista ja niiden levityskampanjoista.

Hyökkääjät eivät hyödy hunajapurkeista, mutta hyökkääjien toiminnasta voidaan silti kerätä tärkeää tietoa. Hunajapurkin rakentamisessa on pyrittävä rakentamaan siitä houkutteleva, eli ottaa käyttöön palveluita, jotka viittaavat kiinnostaviin ominaisuuksiin sekä tehdä hunajapurkista mahdollisimman aidon oloinen.

5.1 Hunajapurkkien tavoite

Verkkoon julkaistujen hunajapurkkien tavoitteena oli tutkia tuotanto- ja teollisuusverkkoihin kohdistettuja hyökkäyksiä julkisessa verkossa. Hunajapurkit keräsivät lokeja niiden portteihin tulleista yhteysyrityksistä.

Huomioitava on, että hunajapurkit olivat Amazonin EC2-pilvipalvelussa, jolloin ne saivat Amazonin omistamalta IP-alueelta julkisen IP-osoitteen. Nämä IP-alueet ja -osoitteet ovat hyvin tunnettuja ja niitä skannataan aktiivisesti, niin hyökkääjien kuin tietoturvatoimijoiden toimesta. Hyvin tunnettu IP-osoite mitä luultavimmin vaikutti järjestelmien nopeaan löytämiseen sekä niihin otettujen yhteyksien määrään.

Toinen huomioitava asia on, että hunajapurkit eivät olleet sijoitettuna sisäverkkoon vaan ne olivat kytketty suoraan julkiseen verkkoon. Haavoittuvan verkon rakentaminen, jonka kautta on pääsy tuotanto- ja teollisuusverkkoon ja sen laitteisiin, olisi vaatinut reilusti enemmän resursseja ja hyökkäyksien määrä olisi mitä luultavimmin tipahtanut huomattavasti.

Hunajapurkit jäljittelivät Siemens SIMATIC S7-200-logiikkakontrolleria ja niissä oli auki yleisesti tunnettuja portteja sekä hieman harvinaisempia portteja. Kaikki portit liittyivät logiikkakontrollerin toimintaan. Hunajapurkeissa oli auki seuraavanlaiset portit:

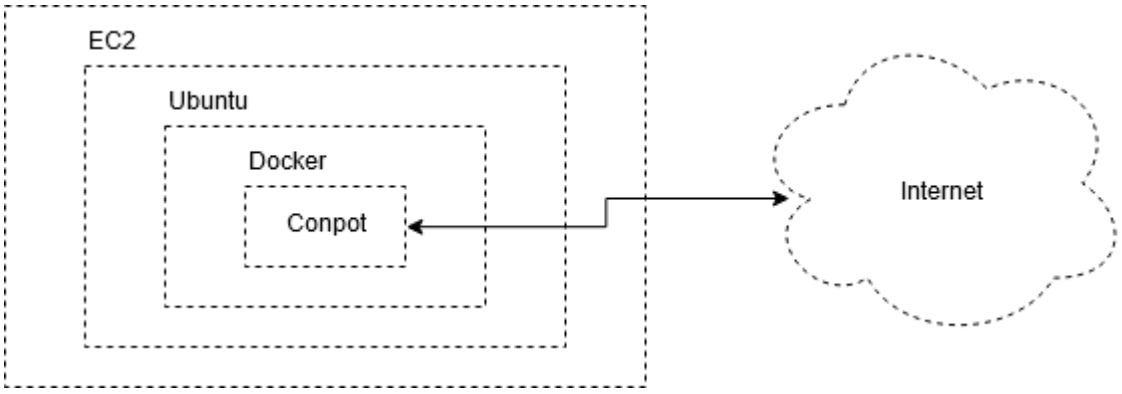
- 21
- 22
- 69
- 80
- 102
- 161
- 502
- 623
- 44818
- 47808.

Realistisemmassa järjestelmässä logiikkakontrolleri olisi ollut löydettävissä vasta hyökkääjän päästyä tunkeutumaan organisaation verkkoon. Tällä kertaa kokonaisen verkon rakentaminen jätettiin tekemättä, sillä tarkoituksena oli kerätä vain tietoa julkisessa verkossa järjestelmään otetuista yhteyksistä sekä niiden määrästä.

5.2 Käytetyt ohjelmistot ja työkalut

Hunajapurkkeja oli yhtäaikaisesti kolme, joista jokainen esitti samanlaista logiikkakontrolleria. Hunajapurkit asennettiin ja otettiin käyttöön täsmälleen samanlaisilla konfiguraatioilla, jotta niiden näkyvyyttä ja hyökkäysten määrää voidaan vertailla mahdollisimman tarkasti. Ne oli sijoitettu eri maanosiin, joka onnistui helposti Amazonin EC2-pilvipalvelulla, sillä Amazon tarjoaa palvelintilaa monesta eri maasta. Ensimmäinen hunajapurkki oli sijoitettu Yhdysvaltoihin, toinen Saksaan ja kolmas Intiaan.

Hunajapurkkeja varten julkaistiin kolme palvelinta, jotka olivat identtisiä. Kuvassa 17 on esitettynä hunajapurkkien julkaisuympäristö, jossa käyttöjärjestelmänä toimi Ubuntu.



Kuva 17. Hunajapurkin julkaisuympäristö.

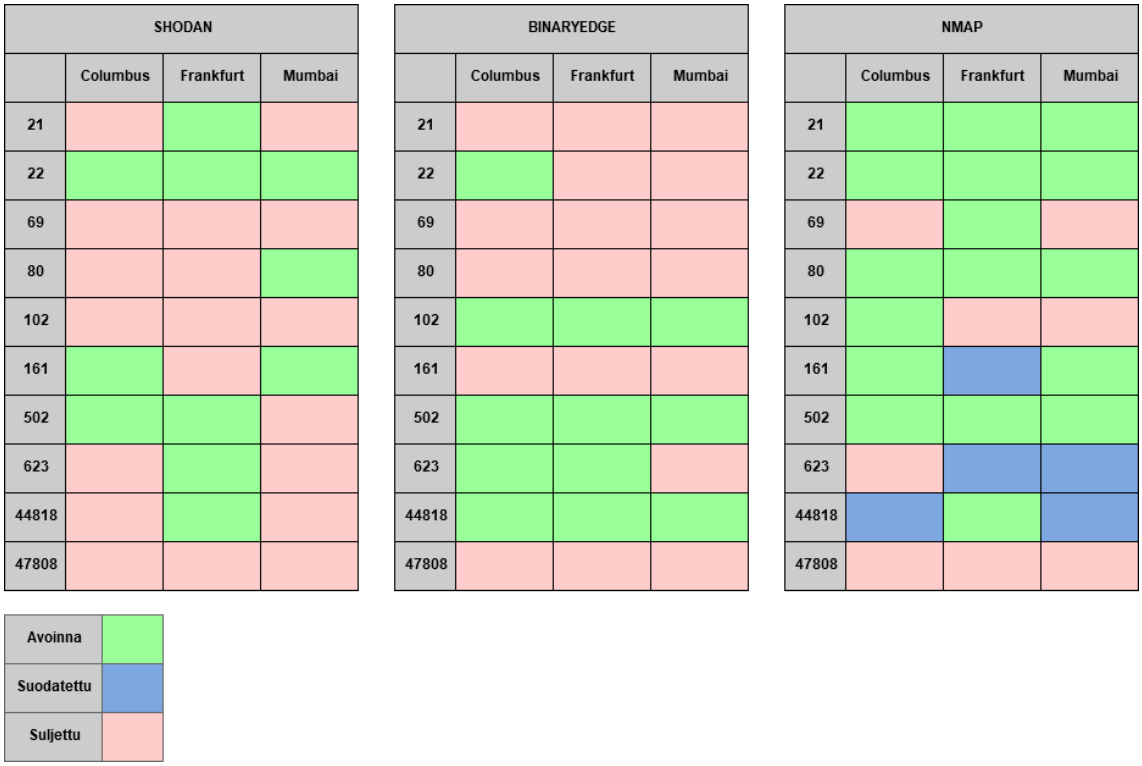
Palvelimille tehtiin laajat palomuuriavaukset Amazonin EC2-palvelun kautta. Jokaiselle palvelimelle asennettiin Docker, jonka sisällä hunajapurkkiohjelmistoa ajettiin. Docker on nopea ja kevyt virtuaaliympäristö, jota käyttämällä erotettiin hyökkäyksen kohteena oleva virtualisoitu logiikkakontrolleri isäntäpalvelimesta. Virtuaaliympäristö Dockerin sisällä ajettiin Conpot -hunajapurkkiohjelmistoa, johon kaikki palvelimelle tullut liikenne ohjattiin.

5.3 Tulokset

Kun hunajapurkit olivat olleet verkossa kaksi viikkoa, olivat ne kaikki jo indeksoituneet Shodan sekä BinaryEdge palveluihin. Shodan sekä BinaryEdge ovat hakukoneita, jotka indeksoivat verkkoon liitettyjä laitteita. Hakukoneilla voi hakea verkkoon kytkettyjä laitteita erilaisilla hakutermeillä, esimerkiksi porttinumeroilla, laitteessa toimivan palvelun nimellä tai versiolla ja lukuisilla muilla hakutermillä.

Hunajapurkit skannattiin myös Nmap-verkkoskannerilla, jota käytetään yleisesti kokonaisten verkkojen ja verkkolaitteiden porttien skannaamiseen. Nmap on hyvin tunnettu työkalu, jonka ajaminen on usein ensimmäisiä vaiheita hyökkäyksen tai penetraatiotestauksen tiedonkeruuvaihetta. Hunajapurkit skannattiin Nmapilla, jotta voitiin vertailla hakukoneiden indeksoimia tuloksia skannaustyökalun tuloksiin.

Kuvassa 18 on esitettynä verkkolaitehakukoneiden sekä Nmapin tulokset avoimista, suodatetuista sekä suljetuista porteista.



Kuva 18. Hunajapurkin portit.

Kumpikaan hakukone ei tunnistanut kaikkia portteja avoimiksi eikä edes Nmap onnistunut tunnistamaan jokaista porttia avoimeksi. Nmapilla tulokset olivat silti parhaimmat, joka ei sinänsä yllättänyt, sillä se on porttien skannaukseen kehitetty työkalu, jonka avulla voidaan suorittaa intensiivisiäkin porttiskannauksia. Lähtökohtaisesti hyökkääjälle riittää, jos verkkolaite on indeksoitu hakupalveluun, sillä näin kohde voidaan löytää nopeasti. Kohteen löytämisen jälkeen voidaan porttiskannaus tehdä tarkemmin esimerkiksi Nmapia käyttäen. Tässä tapauksessa kaikki kolme hunajapurkkia löytyivät hakukoneiden kautta ja erillisellä porttiskannaustyökalulla onnistuttiin saamaan vielä lisätietoa kohteesta.

Shodan indeksoi vain portin 22 kaikista hunajapurkeista. Portti 22 on varattu SSH-palvelulle, joka on hyvin yleinen verkkolaitteiden ja palvelimien etähallintaan käytetty ohjelma ja portti 22 on verkkolaitteissa hyvin usein auki. Mielenkiintoisinta oli kuitenkin, että Shodanin tuloksissa portti 80 oli merkitty avoimeksi vain yhdessä hunajapurkissa. Portti 80 on varattu HTTP-protokollalle, eli verkkosivut ovat saatavilla tästä portista. Hunajapurkkeihin tuli paljon liikennettä porttiin 80, joka on ristiriidassa portin huono indeksoitumisen kanssa Shodaniin.

BinaryEdge indeksoi selvästi tasaisemmin samoja portteja avoimiksi kaikista hunajapurkeista. Portit 102, 502 ja 44818 oli havaittu kaikissa hunajapurkeissa avoimiksi, portti 623 oli havaittu kahdessa avoimeksi ja portti 22 vain yhdessä. Kaikki muut portit olivat palvelun mukaan suljettuja tai hakupalvelulla ei ollut tietoa niiden tilasta. Mielenkiintoa herättää jälleen portti 80, jota BinaryEdge ei ollut tunnistanut yhdessäkään hunajapurkissa avoimeksi. Myöskin portin 22 tunnistaminen avoimeksi vain yhdessä kolmesta kohteesta herättää huomiota, sillä BinaryEdge tunnisti paljon harvinaisempia portteja yhdenmukaisesti kaikissa kohteissa avoimiksi.

Nmap-työkalua käyttäen saatiin paljon laajempia tuloksia avoimista porteista. Kaikki portit läpikäyvällä porttiskannauksella ei kuitenkaan saatu tuloksia, jossa jokainen portti olisi tunnistettu avoimeksi. Luultavasti skannauksen intensiivisyyttä nostamalla olisivat kaikki avoimet portit onnistuttu löytämään. Tulokset olivat jo hyviä lyhyemmällä skannauksella, joten kohteisiin ei enää tarvinnut ajaa intensiivistä skannausta. Viisi porttia oli myös merkitty suodatetuksi Nmapin tuloksissa. Suodatettu portti tarkoittaa, että sen tilasta ei ole tarkkaa tietoa, sillä sen tilaa ei pystytty varmistamaan.

Kaikki kolme hunajapurkkia tulivat indeksoiduiksi Shodan sekä BinaryEdge palveluihin nopeasti, mutta kumpikaan palvelu ei tunnistanut enempää avoimia portteja vielä kahden viikon aikana.

Kolmannen viikon aikana palveluihin kohdistunut liikenne väheni merkittävästi ja Shodanin HoneyScore palvelu oli onnistunut tunnistamaan kaikki kolme palvelinta hunajapurkeiksi. Palvelimiin kohdistuneen liikenteen vähentyessä otettiin kaikki kolme hunajapurkkia pois verkosta ja kerättyjen lokien tarkastelu aloitettiin.

Porttiin 80 (HTTP) otettiin selvästi eniten yhteyksiä, joka johtuu varmasti portin yleisyydestä sekä verkkosovelluksia kohdistavien automaattiskannerien määrästä. Verkkosovellukset ovat useiden hyökkääjien kohteena. Toiseksi eniten liikennettä tuli porttiin 22 (SSH), joka on myös laajojen automaattihyökkäyksien kohteena jatkuvasti. Nämä kaksi porttia keräsivät valtaosan hunajapurkkeihin kohdistuneesta liikenteestä.

Portti 21 (FTP) sai osakseen myös paljon yhteyksiä, mutta ainoa tuotanto- ja teollisuusverkkoihin selvästi viittaava portti, joka sai reilusti liikennettä, oli portti 502 (Modbus). Myös portit 102 (iso-tsap), 623 (ipmi) sekä 44818 (EtherNet-IP-2) keräsivät osakseen jonkin verran liikennettä. Muihin portteihin ei kohdistunut merkittävää määrää liikennettä, vaikka portteja oli indeksoitunut avoimiksi Shodan ja BinaryEdge palveluihin.

6 TIETOTURVAKONTROLLIT

Tuotanto- ja teollisuusverkkojen toimintavarmuuden tueksi on hyvä laatia tietoturvakontrolleja, joilla voidaan määrittää toimintoja verkkojen tietoturvallisuuden sekä hyvän toimintavarmuuden saavuttamiseksi.

Tietoturvakontrollit ovat verkkojen turvallisuuden eteen tehtyjä toimia ja niiden kanssa toimivien henkilöiden toimintamalleja. Kontrollien on tarkoitus auttaa ylläpitämään verkon turvallista toimintaa tarjoamalla turvallisia toimintatapoja sekä ohjeita niin normaaliin käyttöön kuin kriisitilanteisiinkin.

6.1 Prosessin suojaus

Usein organisaatioiden tietoturvassa keskitytään yleisesti suojaamaan omistettua tietoa. Suojattava tieto saattaa olla esimerkiksi käyttäjien tunnustietoja, arkaluontoista asiakasdataa, yrityksen omia tärkeitä dokumentteja tai muuta tallennettua tietoa, joka ei saa päätyä organisaation ulkopuolisten käsiin.

Tuotanto-, ja teollisuusverkot kuitenkin poikkeavat edellä mainitusta, sillä niissä tärkeintä on prosessin suojaaminen. Tuotanto- ja teollisuusverkot ovat kuitenkin hyvinkin erilaisia keskenään, sillä ne usein rakennettaan tarkasti laitoksien tarpeiden mukaisesti. Korkean tason tietoturvakontrolleja voidaan kuitenkin määrittää, joiden käyttöönotossa tulee huomioida tarkemmin kyseisen laitoksen toimintatavat sekä vaatimukset.

Tuotanto- ja teollisuusverkot ovat usein osa laajempaa ympäristöä ja niistä siirretään tietoa monitoroitavaksi ja verkkoihin saattaa tulla ohjausliikennettä. Suurempi tuotantoympäristökokonaisuus voidaankin jakaa kolmeen pienempään kategoriaan:

- Yritysverkko
- Tuotanto- tai teollisuusverkko
- Laiteverkko.

Näistä jokaisen osuuden suojaaminen on oma kokonaisuutensa ja siksi seuraavat tietoturvakontrollit keskittyvätkin yksinomaan tuotanto- ja teollisuusverkkojen suojaamiseen (Knapp & Samani 2013, 114).

6.2 Kontrollit tuotanto- tai teollisuusverkon turvaamiseen

Ensimmäinen asia, joka tulee huomioida tuotanto- tai teollisuusverkon suojaamisessa, on verkkolaitteiden fyysinen turvallisuus. Jos hyökkääjä pääsee laitteisiin fyysisesti käsiksi, voidaan laitteet rikkoa ja siten aiheuttaa haittaa järjestelmän toiminalle. Fyysinen turvallisuus takaa myös, ettei laitteisiin voida liittää muita laitteita tai, että verkkoon ei voi liittää omia laitteita. Ylimääräisten laiteiden kautta verkkoon voi tunkeutua syvemmälle ja aiheuttaa haittaa järjestelmän toiminnalle erilaisten verkkohyökkäysten muodossa.

Huomiota tulee myös kiinnittää verkkoon tuleviin ja siitä lähteviin ulkoisiin yhteyksiin. Tarpeettomat yhteydet tulee sulkea ja tarpeellisten yhteyksien turvallisuus ja toimintatavat tulisi tarkastaa, jotta mahdollisella hyökkääjällä ei ole suoraa reittiä tuotanto- tai teollisuusverkkoympäristöön jo olemassa olevien yhteyksien kautta.

Etähallintayhteyksiin tulee kiinnittää erityistä huomiota, sillä ne ovat yleinen tapa hallita järjestelmän erilaisia laitteita ja ne ovat helposti hyökkääjien kohteina juuri niiden hallintaominaisuuksien vuoksi.

Kaikki verkkolaitteet tulisi koventaa ottamalla tarpeettomat palvelut kokonaan pois käytöstä. Useat oletusasetukset ja -palvelut eivät ole tietoturvan kannalta paras vaihtoehto. Laitteiden asetukset tai konfiguraatio tulisi käydä läpi, etenkin tietoturvaan liittyvät asiat. Täysin tarpeettomat verkkolaitteet tulisi poistaa verkosta kokonaan, sillä ne lisäävät hyökkäyspinta-alaa.

Laitevalmistajien tukemat tietoturvaominaisuudet tulisi ottaa käyttöön, jos vain mahdollista. Laitteiden omat ominaisuudet ovat parhaiten yhteensopivia niiden kanssa, jolloin on helpompi välttyä konfiguraatiovirheiltä. Konfiguraatiovirheet voivat aiheuttaa turvaominaisuuden toimimattomuuden ja pahimmassa tapauksessa jopa luoda uusia haavoittuvuuksia.

Käytettyjen ohjelmistojen päivitykset tulee hoitaa ajallaan. Tuotanto- ja teollisuusverkkoympäristöt ovat usein hankalia päivittää, sillä päivityksien vieminen tuotanto- tai teollisuusympäristöön voi olla haasteellista pelkän verkkoyhteyden yli. Myös päivitysten asentaminen voi olla haastavaa, sillä ympäristöt ovat usein jatkuvasti käytössä ja käyttökatkot tulisi pitää erittäin vähäisinä. Päivitykset saattavat myös rikkoa jo toiminnassa olevan kokonaisuuden, jolloin ne aiheuttavat paljon lisätyötä.

Verkkoympäristön eri osat tulisi testata tai auditoida säännöllisesti tietoturvaongelmien havaitsemiseksi. Havaittujen uhkien korjaamiseen voidaan siten keskittää resursseja ja ne saadaan korjattua nopealla aikataululla.

Iso rooli tuotanto- ja teollisuusverkoissa on niissä käytetyillä protokollilla, sillä verkkojen käyttötarkoitus eroaa reilusti muista tietoverkoista. Tuotanto- ja teollisuusympäristöissä käytetyt protokollat ovat vanhoja, mutta niiden uusimpia versioita voidaan käyttää TCP/IP-verkoissa, ja protokollien paketteja voidaan lähettää saman tietoverkon yli kuin muutakin verkkoliikennettä.

Kun tuotanto- ja teollisuusverkkoliikenne on muun verkkoliikenteen lomassa, nousee liikenteen salaus sekä autentikointi erittäin tärkeään rooliin. Tuotanto- ja teollisuusverkkoliikenne tulisi myös segmentoida omaan verkkoonsa. Kuten testiympäristössä huomattiin, voitiin verkkoliikennettä tarkastella, sillä sitä ei ollut salattu millään tavalla. Salauksen puute mahdollisti tiedon keräämisen ympäristöstä. Autentikoinnin puute taas mahdollisti ala-aseman lähettämän tiedon muuttamiseen, sillä ala-asema ei varmista tiedon lähdettä millään tavalla.

Jo pelkkä salauksen lisääminen tuotanto- tai teollisuusverkkoympäristöön lisää verkkoliikenteen turvallisuutta, sillä hyökkäyksen suorittamiseksi tarvittiin selkokielisestä liikenteestä kerättyjä tietoja. Lisäksi liikenteen lähettäminen laitteelle ei onnistuisi, ellei sitä salattaisi samalla tavalla. Tietoa saatetaan pystyä keräämään myös porttiskannauksella, riippuen laitteen konfiguraatiosta. Palvelujen nimiä ja versiotietoja tulisi piilottaa, jotta tietojen kerääminen järjestelmästä ei olisi niin helppoa.

Autentikoinnin lisääminen tuotanto- tai teollisuusverkkoympäristöön tarkoittaa, että laitteet voivat varmistaa keskustelevansa oikean laitteen kanssa. Tällöin arvoja manipuloivat hyökkäykset eivät onnistu ja tuotanto- tai teollisuusympäristön häiritseminen tällä tavoin on vältetty.

LOPUKSI

Opinnäytetyön tavoitteena oli tutustua tuotanto- ja teollisuusverkkojen toimintaan, niissä yleisesti käytettyihin Modbus, DNP3 sekä IEC 60870-5-104 protokolliin ja tuotantoympäristöjen verkkolaitteisiin. Tarkoitus oli myös tutustua tietoturvatestauksen teoriaan ja testata Modbus-protokollaa käytännössä. Opinnäytetyössä käytiin myös läpi tunnettuja hyökkäyksiä tuotanto- ja teollisuusverkkoja vastaan sekä kerättiin oikeaa tuotantolaitteisiin kohdistuvaa hyökkäysliikennettä.

Soveltava osuus sisälsi virtuaaliympäristön testauksen, jota suoritettaessa noudatettiin penetraatiotestausmallia. Testauksessa oletettiin, että hyökkääjä on jo päässyt tuotantoympäristöön, ja testauksen kohteena oli virtuaaliympäristön käyttämä verkkoprotokolla. Mallia noudattamalla voitiin tarkkailla penetraatiotestauksen etenemistä vaiheittain.

Tuotantolaitteisiin kohdistuvan hyökkäysliikenteen kerääminen oli myös osana soveltavaa osuutta. Hyökkäysliikenteen keräämisessä huomioon otettavaa oli, että hunajapurkki sai julkisen IP-osoitteen Amazonilta, joka varmasti vaikutti hyökkäysliikenteen määrään heti alussa.

Teorian sekä käytännön osuuksien pohjalta laadittiin tietoturvakontrolleja tuotanto- ja teollisuusympäristöjen koventamiseen. Tietoturvakontrollit ovat pitkälti samanlaisia kuin minkä tahansa verkkoympäristön tietoturvakontrollit, erona protokollien käyttöön liittyvät seikat sekä verkon segmentoinnin tärkeys.

Uskon, että tuotanto- ja teollisuusverkkojen tietoturvaan tullaan kiinnittämään paljon huomioita lähitulevaisuudessa. Tietoturva on jatkuvasti puheenaiheena ja erityisesti yhteiskunnan kannalta kriittisten laitoksien tulee noudattaa hyviä tietoturvakäytäntöjä.

LÄHTEET

Ars Technica 2012. Confirmed: US and Israel created Stuxnet, lost control of it. Viitattu 20.11.2019. Saatavilla sähköisesti osoitteessa https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/.

Bailey, D. & Wright, E. 2003. Practical SCADA for Industry. Iso-Britannia: IDC Technologies.

Barnum, S.; Gegick, M. & C.C., M. 2005. Defense in Depth. Viitattu 12.11.2019. Saatavilla sähköisesti osoitteessa https://www.us-cert.gov/bsi/articles/knowledge/principles/defense-in-depth.

Clarke, G.; Reynders, D. & Wright, E. 2004. Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems. Iso-Britannia: IDC Technologies.

DNP Users Group. 2005. A DNP3 Protocol Primer. Viitattu 11.11.2019. Saatavilla sähköisesti osoitteessa https://www.dnp.org/Portals/0/AboutUs/DNP3%20Primer%20Rev%20A.pdf.

Knapp, Eric. & Samani, R. 2013. Applied Cyber Security and the Smart Grid. Yhdysvallat: Elsevier Inc.

Modbus Organization. 2012. Modbus Application Protocol. Viitattu 12.11.2019. Saatavilla sähköisesti osoitteessa http://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf.

Norton 2019. What is a honeypot? How it can lure cyberattackers. Viitattu 10.10.2019. Saatavilla sähköisesti osoitteessa https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html.

OPC Foundation 2019. Classic. Viitattu 14.10.2019. www.opcfoundation.org > About > OPC Technologies > Classic

OPC Foundation 2019. UA Companion Specifications. Viitattu 14.10.2019. www.opcfoundation.org > About > OPC Technologies > UA Companion Specifications

OPC Foundation 2019. Unified Architecture (UA). Viitattu 14.10.2019. www.opcfoundation.org > About > OPC Technologies > Unified Architecture (UA)

OPC Foundation 2019. What is OPC? Viitattu 14.10.2019. www.opcfoundation.org > About > What is OPC?

PTES 2019. Exploitation. Viitattu 19.10.2019. www.pentest-standard.org/index.php > Exploitation

PTES 2019. Intelligence Gathering. Viitattu 17.10.2019. www.pentest-standard.org/index.php > Intelligence Gathering

PTES 2019. Post Exploitation. Viitattu 19.10.2019. www.pentest-standard.org/index.php > Post Exploitation

PTES 2019. Pre-engagement Interactions. Viitattu 15.10.2019. www.pentest-standard.org/index.php > Pre-engagement Interactions

PTES 2019. Threat Modeling. Viitattu 17.10.2019. www.pentest-standard.org/index.php > Threat Modeling

PTES 2019. Vulnerability analysis. Viitattu 18.10.2019. www.pentest-standard.org/index.php > Vulnerability Analysis

STF 2019. Black Box Testing. Viitattu 12.10.2019. www.softwaretestingfundamentals.com > Software Testing Methods > Black Box Testing

STF 2019. Gray Box Testing. Viitattu 12.10.2019. www.softwaretestingfundamentals.com > Software Testing Methods > Gray Box Testing

STF 2019. White Box Testing. Viitattu 12.10.2019. www.softwaretestingfundamentals.com > Software Testing Methods > White Box Testing

Stouffer, K.; Pilliteri, V.; Lightman, S.; Abrams, M. & Hahn, A. 2015. Guide to Industrial Control Systems (ICS) Security. Yhdysvallat: National Institute of Standards and Technology.

The Penetration Testing Execution Standard (PTES) 2019. Main page. Viitattu 15.10.2019. www.pentest-standard.org/index.php/Main_Page

We Live Security 2016. BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry. Viitattu 20.11.2019. Saatavilla sähköisesti osoitteessa https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/.

Weed. S. 2017. US Policy Response to Cyber Attack on SCADA Systems Supporting Critical National Infrastructure. Viitattu 16.10.2019. Saatavilla sähköisesti osoitteessa https://media.defense.gov/2017/Nov/20/2001846609/-1/-1/0/CPP0007_WEED_SCADA.PDF.