TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

MIKAEL ERIKSSON

ASE-6010 TIETOVERKKOPOHJAINEN AUTOMAATIO

Harjoitustyö 2

SISÄLLYSLUETTELO

.

1. JOHDANTO

Harjoitustyön tarkoituksena oli tuottaa raportti kurssin ASECyberLab-tietokoneharjoituksista 3 ja 4. Harjoitusten yhteisenä tavoitteena oli muodostaa mahdollisimman selkeä käsitys tutkittavasta ICS-verkkosegmentistä ja listata verkosta löytyneet käyttöjärjestelmät, laitteet, ohjelmistot, versionumerot ja haavoittuvuudet.

Päällimmäisenä tavoitteena oli kuitenkin tutustua valittuihin työkaluihin ja niiden käyttämiseen. Harjoitukset toteutettiin tietokoneluokassa Windows-ympäristöön asennetulla, ICS-verkkoon kytketyllä BackBox-virtuaalikoneella. Käytetyt työkalut on esitelty omissa alakappaleissaan osana johdantoa, verkon rakenne, laitteet ja liikenne myöhemmin omissa kappaleissaan.

1.1 NMAP/ZenMAP

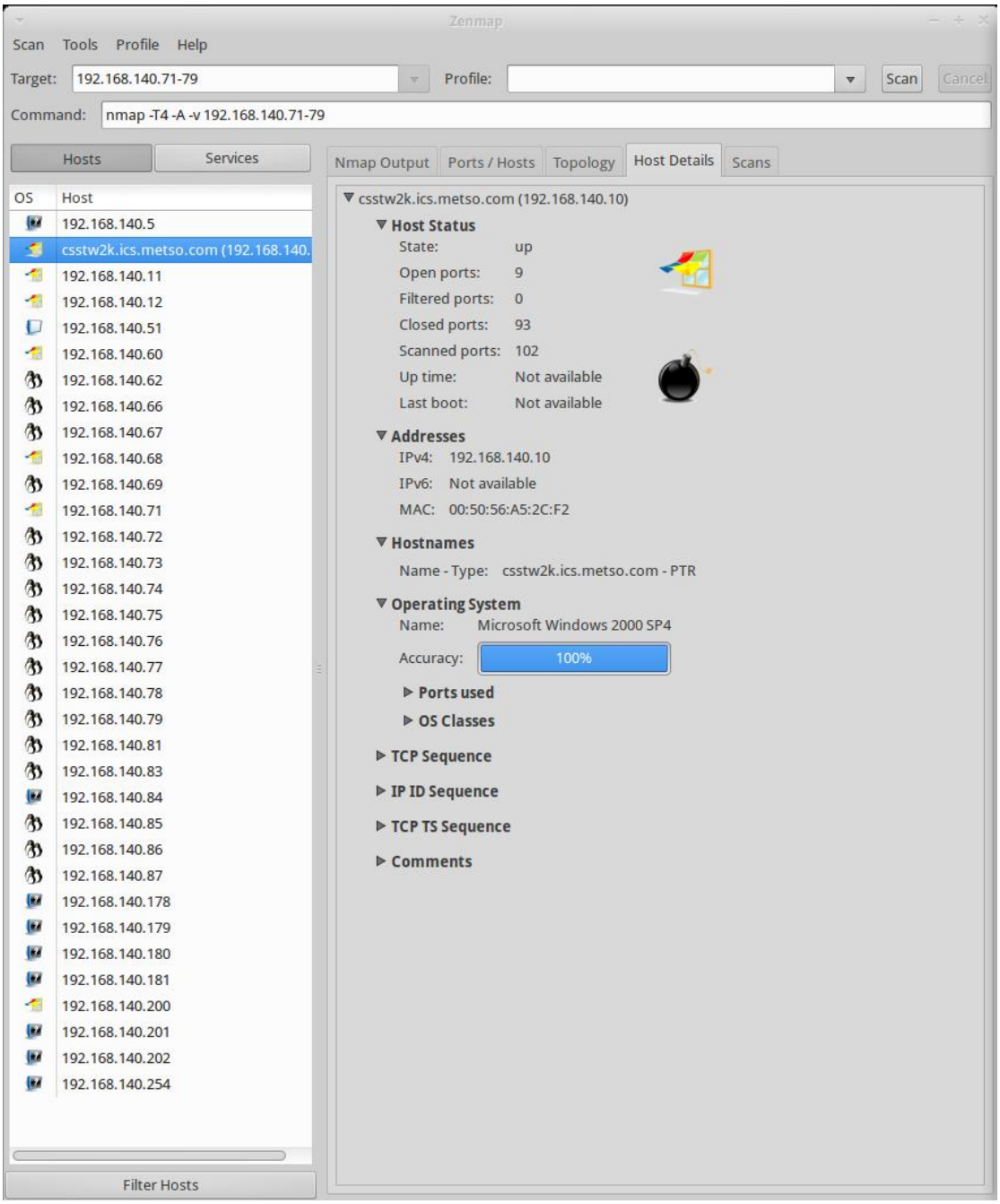
Nmap on verkon tutkimiseen tarkoitettu ohjelmisto. Sitä käytetään verkon hostien ja palveluiden löytämiseen luomaan kuva verkon topologiasta. Nmap lähettää verkon hosteille erilaisia, varta vasten luotuja paketteja ja analysoi näiltä saatuja vastauksia. Tällä tavoin Nmap selvittää esimerkiksi verkon laitteiden käyttöjärjestelmät ja avoimet portit. Tärkeimpiä ominaisuuksia ovat:

- Host Discovery
- Port Scanning
- Version Detection
- OS Detection

[1]

Nmap on alunperin Linux-ympäristöön tehty ohjelmisto, mutta se on nykyään saatavilla myös esimerkiksi Windowsille ja erinäisille UNIX-pohjaisille käyttöjärjestelmille. [1]

Zenmap on Nmapin virallinen graafinen käyttöliittymä. Se on ilmainen ja tukee useita käyttöjärjestelmiä, kuten Linux, Windows ja Mac OS X. Sen tarkoituksena on helpottaa Nmapin käyttöä aloittelijoille, mutta tarjoaa myös vaativammat operaatiot kokeneille käyttäjille. [2]



Kuva 1. Zenmap-käyttöliittymä

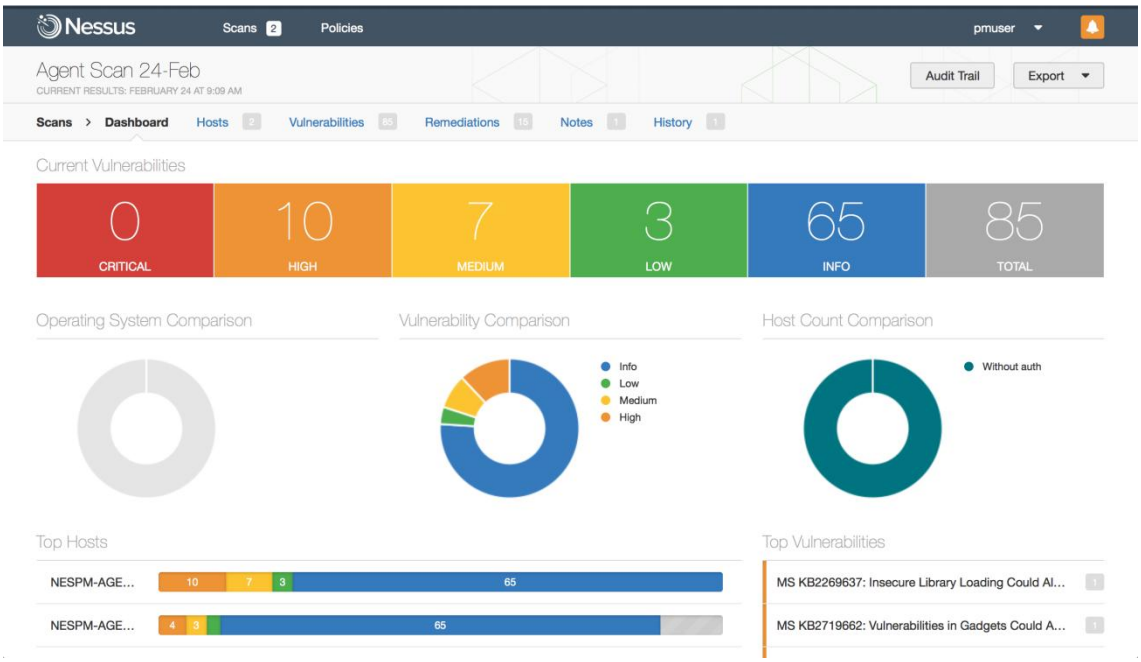
Kuvassa 1 on esitetty Zenmap-käyttöliittymä. Käyttöliittymän yläreunassa näkyvään Target-kenttään syötetään haluttu IP-avaruus, jolle Command-kenttään syötetyt komennot suoritetaan. Kuvan vasemmassa reunassa valkealla pohjalla näkyy listattuna laitteet, jotka löydettiin samasta verkosta harjoituksessa 3. Näkymän oikealla puolella harmaalla pohjalla on esitettynä ohjelman löytämät tiedot eräästä verkossa olleesta laitteesta.

1.2 NESSUS

Nessus on Tenable Network Securityn kehittämä ohjelmisto, jonka tehtävänä on selvittää verkkolaitteiden haavoittuvuuksia. Sillä voidaan kartoittaa esimerkiksi DoS-hyökkäksen tai etähallinnan mahdollistavia haavoittuvuuksia ja oletussalasanojen käyttöä. [3]

Ensin Nessus suorittaa porttiskannauksen selvitääkseen, mitkä laitteen porteista ovat auki. Tämän jälkeen se suorittaa avoimille portteille joukon erinäisiä testejä selvittääkseen, onko niitä mahdollista käyttää hyväksi. Normaalisti Nessus suorittaa laitteille vain turvallisia testejä, mutta käyttäjä voi halutessaan antaa ohjelmalle luvan kokeilla, saako laitteen kaatumaan jollain käytössä olevista testeistä. [3]

Nessuksen käyttöliittymä toimii webselaimella, jonka kautta ohjelma myös esittää raportin löydetyistä haavoittuvuuksista. Tulokset voidaan myös tulostaa esimerkiksi pdf-muotoon. [3]



Kuva 2. Nessus-webkäyttöliittymä [5]

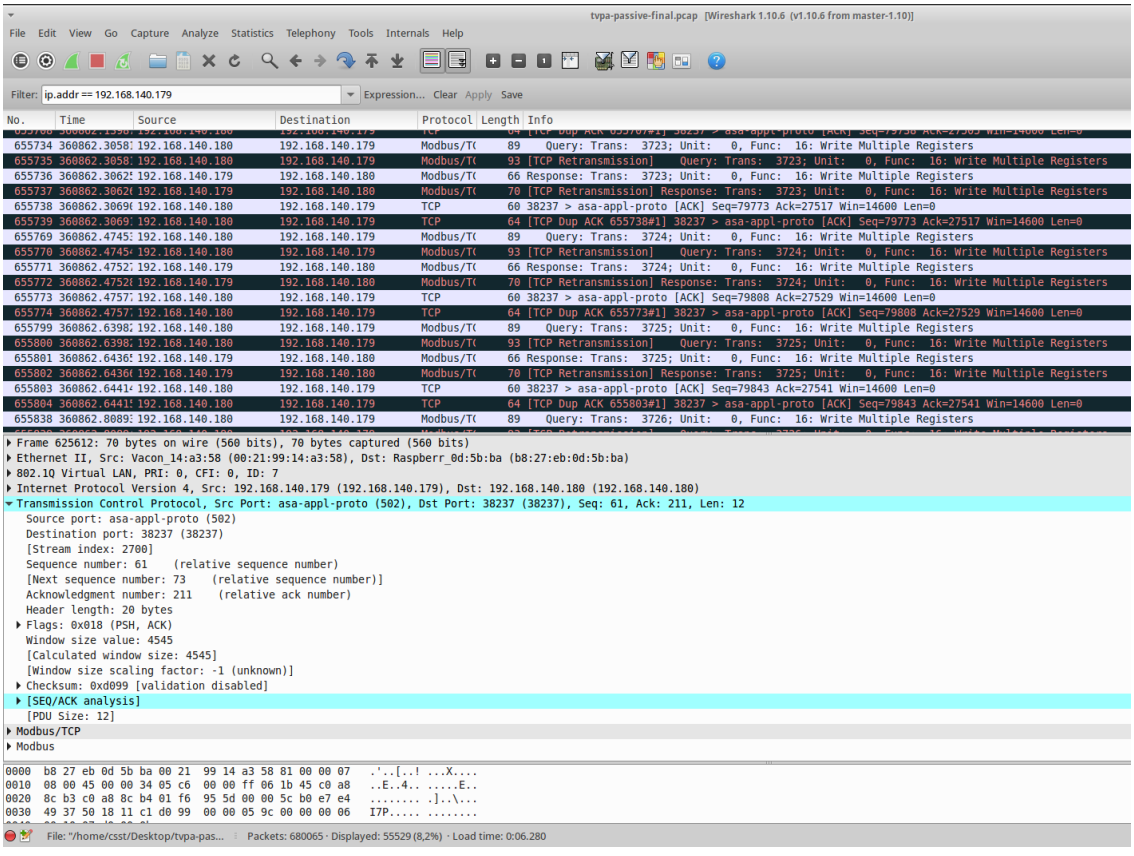
Kuvassa 2 on esitettynä Nessus-käyttöliittymän Dashboard, jossa on näkyvillä tulokset suoritetusta Agent Scannista. Käyttöliittymä esittää graafisen, värikoodatun yhteenvedon löydetyistä haavoittuvuuksista. Kuva on osa Tenable Network Securityn markkinointimateriaalia.

Tenable Network Security julkaisee Nessukselle kymmeniä uusia haavoittuvuustestejä viikossa ja Nessus on yksi maailman käytetyimmistä haavoittuvuusskannereista. Nessus on yksityiskäyttöön ilmainen. [3, 4]

1.3 Wireshark

Wireshark on ilmainen avoimen lähdekoodin ohjelma verkkoliikenteen analysointiin. Se on eräs suosituimmista työkaluista esimerkiksi verkon analysointiin, verkko-ongelmien ratkaisemiseen ja tietoliikenneprotokollien kehittämiseen. Ohjelma osaa lukea esimerkiksi Ethernet, IEEE 802.11 ja PPP –verkkojen liikennettä ja se on saatavilla useille eri käyttöjärjestelmille, kuten Windows, Linux ja MAC OS X. [6]

Wireshark ymmärtää eri verkkoprotokollien rakenteet; sen avulla voidaan kaapata ja lajitella verkossa liikkuvat paketit esimerkiksi protokollan mukaan. Verkkoliikenne voidaan kaapata suoraan lennosta tai lukea aiemmin tallennetut paketit tiedostosta. Kaapattua dataa voidaan lajitella erilaisten suodattimien avulla ja Wireshark osaa esimerkiksi kaapata ja toistaa VoIP-puhelun lennosta, jos pakkausalgoritmi on tunnettu. Tiedon käsittely tapahtuu Wiresharkin graafisen käyttöliittymän kautta tai komentorivillä ohjelman TShark-versiolla. [6]

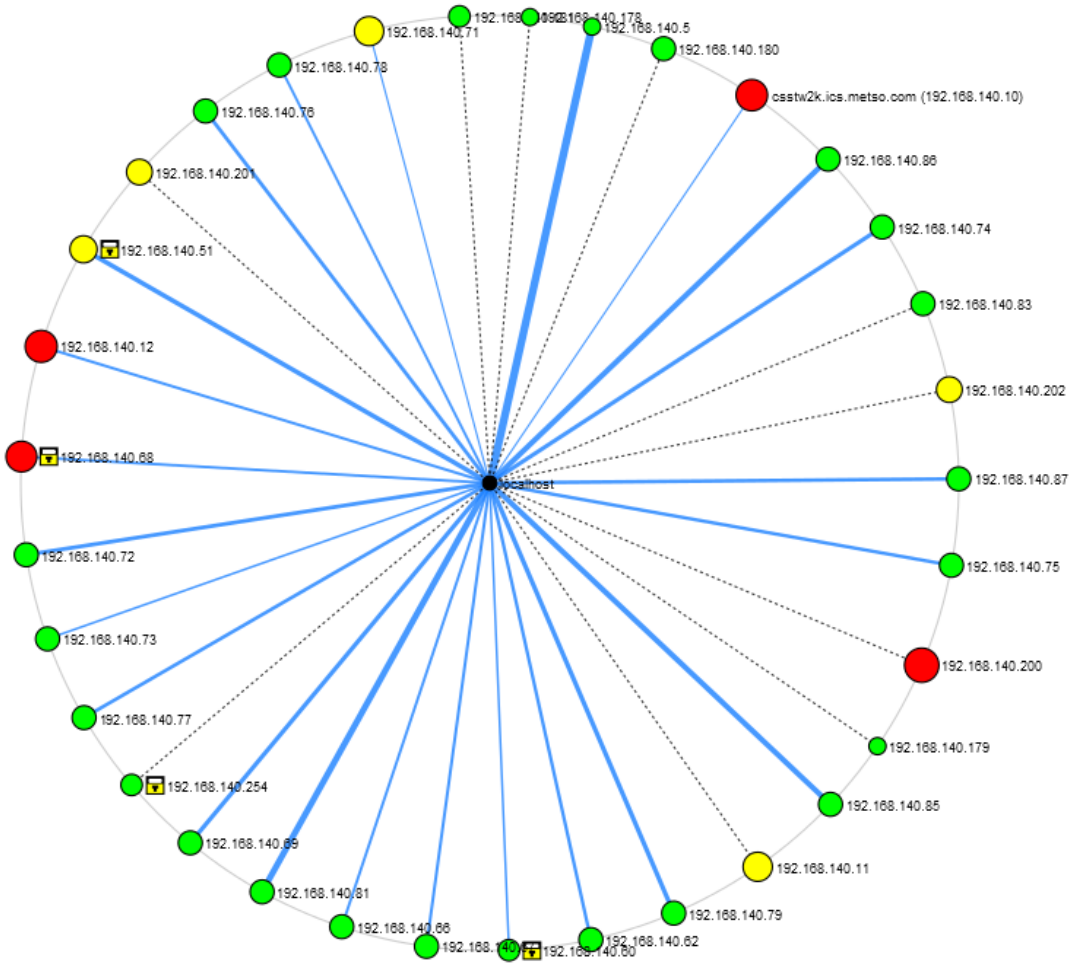


Kuva 3. Wireshark-käyttöliittymä.

Kuvassa 3 on esitetty Wireshark-käyttöliittymä, jossa on näkyvillä harjoituksessa 3 tutkittua verkkoliikennettä. Lista kaapatuista paketeista on esillä päänäkymän yläosassa (raidallinen osio), jossa näkyy paketin numero, aika, lähettäjä, vastaanottaja, pituus, protokolla ja info-osio. Listan alapuolella on esillä erään listasta valitun paketin sisältö.

Ylhäällä vasemmalla näkyvään Filter-kenttään on syötetty suodattimeksi ”ip.addr == 192.168.140.179”, jolloin ohjelma näyttää käsiteltävästä datasta vain kyseisen IP-osoitteen lähettämät ja vastaanottamat paketit. Wireshark tarjoaa runsaasti erilaisia suodatusvaihtoehtoja ja niiden käyttö on etenkin normaalia verkkoliikennettä tutkiessa käytännössä välttämätöntä.

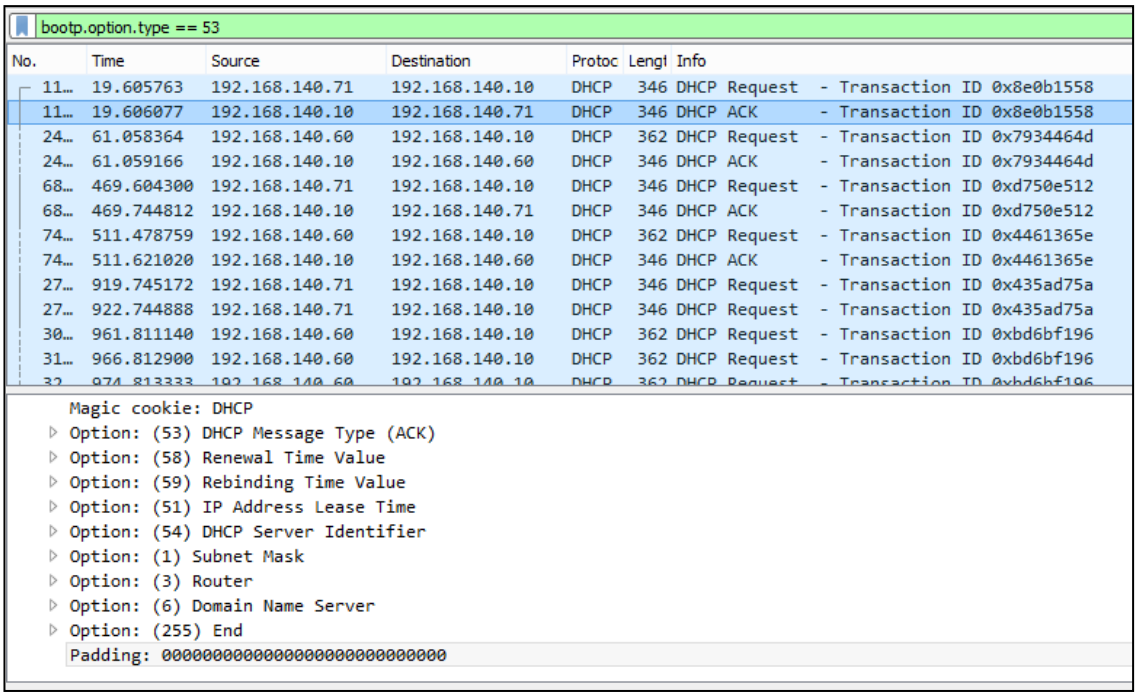
2. VERKON YLEINEN RAKENNE



Kuva 4. Verkon topologia

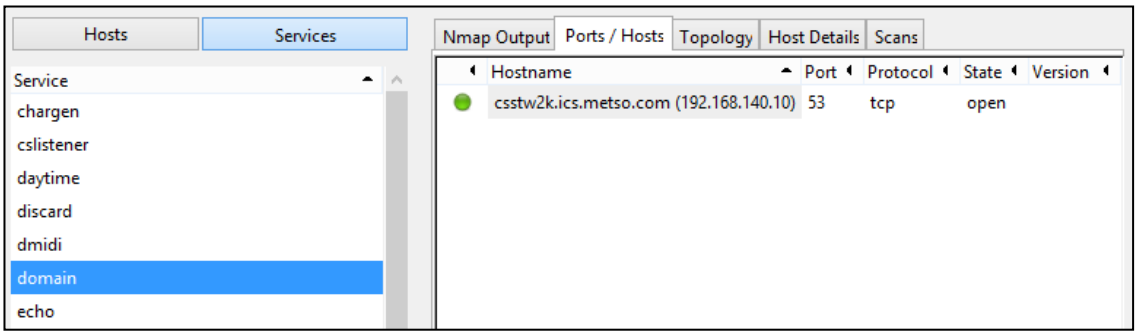
Kuvassa 4 on esitettynä Zenmapin näkemys tutkitun ICS-verkon topologiasta. Ympyrän kehällä olevat pallot esittävät verkon hosteja. Pallon koko ja väri kuvastavat avoimien porttien lukumäärää. Vihreällä pallolla merkityillä hosteissa avoimia portteja on alle kolme, keltaisilla kolmesta kuuteen ja punaisilla yli kuusi. Keskenään samanvärisistä palloista suuremmalla on enemmän avoimia portteja, kuin pienemmällä. Pallon yhteydessä esiintyvä lukon kuva kertoo, että osa hostin porteista on filtteröity. [7]

Verkon liikennettä Wiresharkilla tutkiessa saadaan selville DHCP-palvelin. Kaapattu data voidaan kuvan 5 mukaisesti suodattaa filtterillä ”bootp.option.type == 53”, jolloin esille jää vain DHCP-viestit. DHCP-palvelimen voi tunnistaa sille osoitetuista DHCP Request -viesteistä ja sen lähettämistä DHCP ACK –viesteistä.



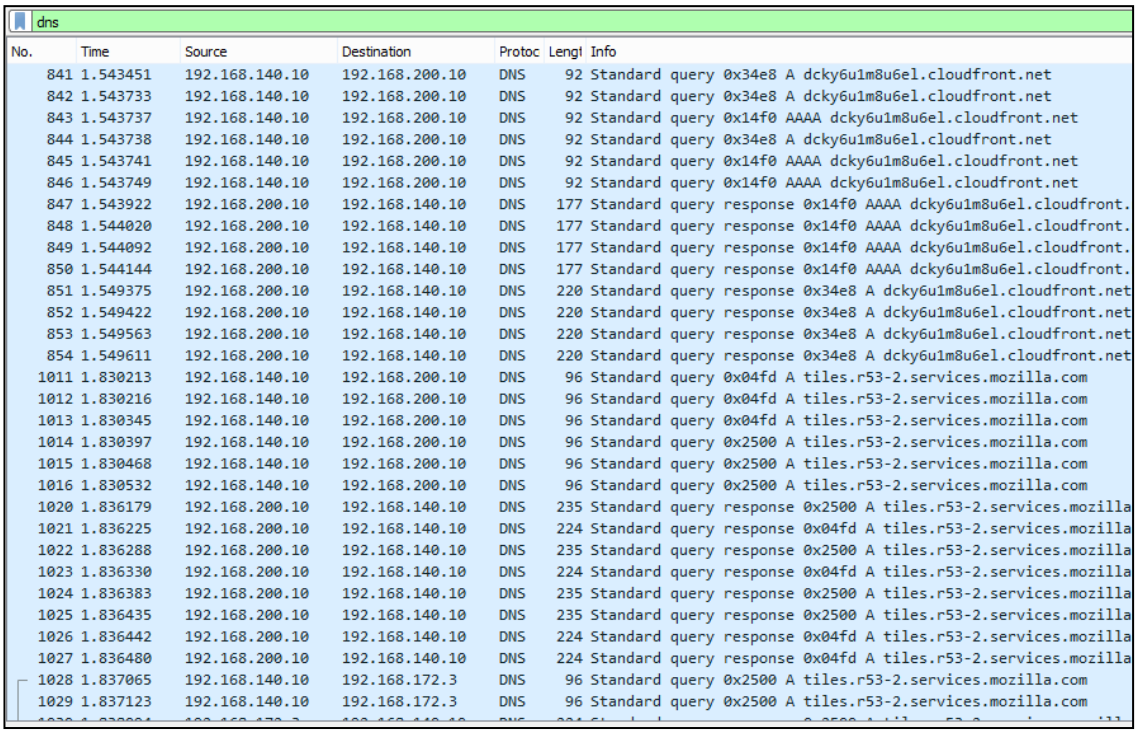
Kuva 5. Wiresharkilla verkosta kaapattuja DHCP-viestejä

Kaapattuja paketteja tutkittaessa huomataan, että DHCP ACK -viestejä verkossa lähettää vain yksi laite, IP 192.168.140.10. DHCP-palvelin löytyy myös Zenmapilla tehdystä skannauksesta, kuten kuvasta 6 nähdään.



Kuva 6. Zenmapin verkosta löytämä domain-palvelu

Sama laite toimii myös paikallisena nimipalvelimena, DNS Resolverina. Tämä huomataan, kun Wiresharkilla kaapattu liikenne suodatetaan esittämään vain DNS-viestit.



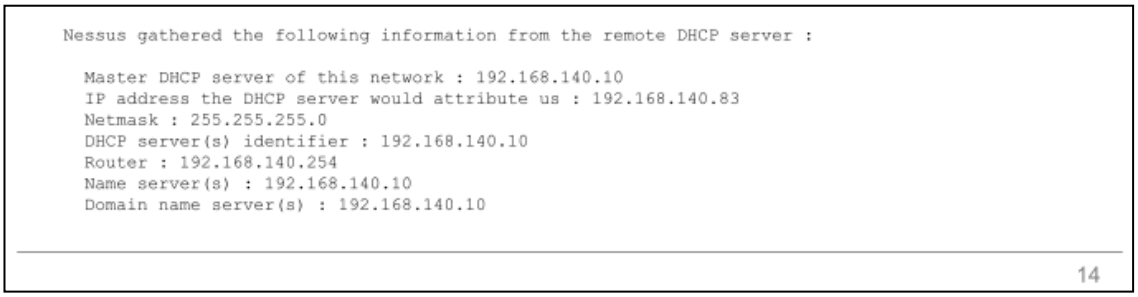
dns

No.	Time	Source	Destination	Protoc	Lengt	Info
841	1.543451	192.168.140.10	192.168.200.10	DNS	92	Standard query 0x34e8 A dcky6u1m8u6el.cloudfront.net
842	1.543733	192.168.140.10	192.168.200.10	DNS	92	Standard query 0x34e8 A dcky6u1m8u6el.cloudfront.net
843	1.543737	192.168.140.10	192.168.200.10	DNS	92	Standard query 0x14f0 AAAA dcky6u1m8u6el.cloudfront.net
844	1.543738	192.168.140.10	192.168.200.10	DNS	92	Standard query 0x34e8 A dcky6u1m8u6el.cloudfront.net
845	1.543741	192.168.140.10	192.168.200.10	DNS	92	Standard query 0x14f0 AAAA dcky6u1m8u6el.cloudfront.net
846	1.543749	192.168.140.10	192.168.200.10	DNS	92	Standard query 0x14f0 AAAA dcky6u1m8u6el.cloudfront.net
847	1.543922	192.168.200.10	192.168.140.10	DNS	177	Standard query response 0x14f0 AAAA dcky6u1m8u6el.cloudfront.
848	1.544020	192.168.200.10	192.168.140.10	DNS	177	Standard query response 0x14f0 AAAA dcky6u1m8u6el.cloudfront.
849	1.544092	192.168.200.10	192.168.140.10	DNS	177	Standard query response 0x14f0 AAAA dcky6u1m8u6el.cloudfront.
850	1.544144	192.168.200.10	192.168.140.10	DNS	177	Standard query response 0x14f0 AAAA dcky6u1m8u6el.cloudfront.
851	1.549375	192.168.200.10	192.168.140.10	DNS	220	Standard query response 0x34e8 A dcky6u1m8u6el.cloudfront.net
852	1.549422	192.168.200.10	192.168.140.10	DNS	220	Standard query response 0x34e8 A dcky6u1m8u6el.cloudfront.net
853	1.549563	192.168.200.10	192.168.140.10	DNS	220	Standard query response 0x34e8 A dcky6u1m8u6el.cloudfront.net
854	1.549611	192.168.200.10	192.168.140.10	DNS	220	Standard query response 0x34e8 A dcky6u1m8u6el.cloudfront.net
1011	1.830213	192.168.140.10	192.168.200.10	DNS	96	Standard query 0x04fd A tiles.r53-2.services.mozilla.com
1012	1.830216	192.168.140.10	192.168.200.10	DNS	96	Standard query 0x04fd A tiles.r53-2.services.mozilla.com
1013	1.830345	192.168.140.10	192.168.200.10	DNS	96	Standard query 0x04fd A tiles.r53-2.services.mozilla.com
1014	1.830397	192.168.140.10	192.168.200.10	DNS	96	Standard query 0x2500 A tiles.r53-2.services.mozilla.com
1015	1.830468	192.168.140.10	192.168.200.10	DNS	96	Standard query 0x2500 A tiles.r53-2.services.mozilla.com
1016	1.830532	192.168.140.10	192.168.200.10	DNS	96	Standard query 0x2500 A tiles.r53-2.services.mozilla.com
1020	1.836179	192.168.200.10	192.168.140.10	DNS	235	Standard query response 0x2500 A tiles.r53-2.services.mozilla
1021	1.836225	192.168.200.10	192.168.140.10	DNS	224	Standard query response 0x04fd A tiles.r53-2.services.mozilla
1022	1.836288	192.168.200.10	192.168.140.10	DNS	235	Standard query response 0x2500 A tiles.r53-2.services.mozilla
1023	1.836330	192.168.200.10	192.168.140.10	DNS	224	Standard query response 0x04fd A tiles.r53-2.services.mozilla
1024	1.836383	192.168.200.10	192.168.140.10	DNS	235	Standard query response 0x2500 A tiles.r53-2.services.mozilla
1025	1.836435	192.168.200.10	192.168.140.10	DNS	235	Standard query response 0x2500 A tiles.r53-2.services.mozilla
1026	1.836442	192.168.200.10	192.168.140.10	DNS	224	Standard query response 0x04fd A tiles.r53-2.services.mozilla
1027	1.836480	192.168.200.10	192.168.140.10	DNS	224	Standard query response 0x04fd A tiles.r53-2.services.mozilla
1028	1.837065	192.168.140.10	192.168.172.3	DNS	96	Standard query 0x2500 A tiles.r53-2.services.mozilla.com
1029	1.837123	192.168.140.10	192.168.172.3	DNS	96	Standard query 0x2500 A tiles.r53-2.services.mozilla.com

Kuva 7. Wiresharkilla kaapattuja DNS-viestejä

Kuvasta 7 huomataan, että 192.168.140.10 lähettää nimikyselyitä ja saa niihin myös vastauksia. Suurin osa laitteen verkkoliikenteestä on DNS-viestejä.

Sama on huomattavissa myös laitteelle suoritetussa haavoittuvuuskartoituksessa, jonka yhteydessä selvisi kuvan 8 mukaiset tiedot.



```
Nessus gathered the following information from the remote DHCP server :

  Master DHCP server of this network : 192.168.140.10
  IP address the DHCP server would attribute us : 192.168.140.83
  Netmask : 255.255.255.0
  DHCP server(s) identifier : 192.168.140.10
  Router : 192.168.140.254
  Name server(s) : 192.168.140.10
  Domain name server(s) : 192.168.140.10
```

14

Kuva 8. Nessus Basic Scan, IP 192.168.140.10

Nessuksen raportissa nähdään myös reitittimen IP-osoite 192.168.140.254.

3. VERKON LAITTEET JA OHJELMISTOT

Tutkitussa verkkosegmentissä oli harjoituksen 3 aikana kaikkiaan 34 laitetta. Suurin osa verkon laitteista on luokan tietokoneilla pyöriviä virtuaalikoneita, joilla suoritetaan samaista verkkoanalyysiä. Alla on lista verkon muista laitteista ja niistä harjoituksissa käytetyillä työkaluilla kerätyt tiedot.

192.168.140.5
MAC Address: 00:C0:F0:05:91:64 (Kingston Technology)

192.168.140.10
MAC Address: 00:50:56:A5:2C:F2 (VMware)
DNS Name: csstw2k.ics.metso.com
Netbios Name: CSST_W2K
OS: Microsoft Windows 2000 Server Service Pack 4

192.168.140.11
MAC Address: 00:50:56:80:31:65 (VMware)
Netbios Name: SCADA
OS: Microsoft Windows XP, Microsoft Windows XP Service Pack 1

192.168.140.12
MAC Address: 00:50:56:80:1B:C7 (VMware)
Netbios Name: S7
OS: Microsoft Windows XP, Microsoft Windows XP Service Pack 1

192.168.140.51
MAC Address: 00:80:2F:15:BD:66 (National Instruments)
OS: Apple Airport, Canon imageRunner Printer, HP Switch, Nortel Switch

192.168.140.60
MAC Address: 00:50:56:A5:13:97 (VMware)
Netbios Name: VACONLIVE
MAC Address: 00:50:56:a5:13:97

192.168.140.68
MAC Address: 00:50:56:A5:15:8E (VMware)
Netbios Name: QUBE8X
OS: Microsoft Windows 8.1 Enterprise

192.168.140.71
MAC Address: 00:50:56:80:08:44 (VMware)
Netbios Name: NT4
OS: Microsoft Windows NT 4.0 Server
192.168.140.178
MAC Address: 00:21:99:14:A9:F0 (Vacon Plc)
OS: KYOCERA Printer

192.168.140.179
MAC Address: 00:21:99:14:A3:58 (Vacon Plc)
OS: KYOCERA Printer

192.168.140.180
MAC Address: B8:27:EB:0D:5B:BA (Raspberry Pi Foundation)
OS: Linux Kernel 3.2 on Debian 7.0 (wheezy)

192.168.140.181
MAC Address: B8:27:EB:AA:58:8B (Raspberry Pi Foundation)

192.168.140.200
MAC Address: 00:50:56:01:01:10 (VMware)
Netbios Name: METSODNA_DEMO
OS: Microsoft Windows 7 Enterprise

192.168.140.201
MAC Address: 00:40:AA:00:D8:34 (Metso Automation)

192.168.140.202
MAC Address: 00:40:AA:00:D8:62 (Metso Automation)

192.168.140.254
MAC Address: 00:50:56:80:7E:22 (VMware)

Nessus-analyysi kerettiin tehdä vain IP-osoitteille välillä 192.168.140.1-200, joten viimeiset kolme laitetta eivät päässeet Nessuksen analysoitavaksi. MAC-osoitteen pohjalta voitaneen todeta 192.168.140.201 ja 192.168.140.202 olevan Metso Automationin laitteita ja 192.168.140.244 on verkon reititin.

4. VERKKOLIIKENNE

Verkkoliikenteen tarkastelussa luokan virtuaalikoneet päätettiin jälleen jättää pois ja suurennuslasin alle otettiin samat laitteet, jotka esiteltiin edellisessä kappaleessa. Wiresharkilla kaapatusta verkkoliikenteestä pyrittiin etsimään jokaiselle laitteelle jokin kyseisen laitteen verkkoliikenteeseen liittyvä erityispiirre.

Tulokset on koottu alle järjestyksessä IP-osoitteen mukaan.

192.168.140.5
Wireshark-kuuntelun aikana ei kaapattu ainuttakaan pakettia.

192.168.140.10
Verkon DNS- ja DHCP-palvelin, joten suurin osa liikenteestä koostuu näistä viesteistä. Kaikkiaan 23035 kaapatusta paketista 275 on muita, kuin DNS-viestejä. Valtaosa jäljelle jäävistä paketeista on NBNS-broadcasteja omaan aliverkkoon.

192.168.140.11
Kaikkiaan 10814 kaapatusta paketista vain 48 on muita, kuin IP-osoitteeseen 239.0.171.1 lähetettyjä UDP-paketteja. Loput liikenteestä on dialogia DNS/DHCP-palvelimen kanssa.

192.168.140.12
Liikenteessä suurin yksittäinen esiintyvä protokolla on lähteviä ja saapuvia DNS-paketteja. Joukosta erottuen mukana myös muutama HTTP-paketti. Nessus havaitsi web-serverin portissa tcp/5000.

192.168.140.51
Ainut laite, joka lähetti PTPv2-viestejä. Kaikissa vastaanottajana 224.0.1.129, PTP-protokollan multicast-osoite.

Kaikkiaan 260 443 paketista 240 708 oli TCP-dialogia 192.168.140.68 kanssa.
Wiresharkilla kaapatusta liikenteestä 38,3% oli kyseisen laitteen lähettämää tai vastaanottamaa.

192.168.140.60
Laite lähetti satunnaisesti joukon HTTP-paketteja osoitteeseen 239.255.255.250 sekä BROWSER, ”Host Announcement VACONLIVE” ja NBNS –broadcasteja omaan lähiverkkoon.

Kaikkiaan 249 816 paketista 201 693 oli TCP-dialogia 192.168.140.178 kanssa ja 47 582 pakettia TCP-dialogia 192.168.140.179 kanssa.
Wiresharkilla kaapatusta liikenteestä 36,7% oli kyseisen laitteen lähettämää tai vastaanottamaa.

192.168.140.68
Laitteen liikenteestä suurin osa dialogia 192.168.140.51 kanssa. Jäljelle jäävistä 156 paketista iso osa on SSDP (HTTP) tai UDP-paketteja vastaanottajana 239.255.255.250.

192.168.140.71
Pääosa 278 paketin liikenteestä on NBNS-broadcasteja, loput 10 DHCP-viestejä.

192.168.140.178
Laitteen liikenteestä suurin osa dialogia 192.168.140.60 kanssa, jäljelle jäävistä 23381 paketista suurin osa TCP ja Modbus/TCP-liikennettä 192.168.140.180.

192.168.140.179
Laitteen liikenteestä suurin osa TCP-dialogia 192.168.140.60 kanssa, jäljelle jäävistä suurin osa TCP ja TCP/Modbus –dialogia 192.168.140.180 kanssa. Vain 6 pakettia muille vastaanottajille, jotka kaikki Membership Report group-paketteja osoitteisiin 224.0.0.1 ja 239.6.53.80.

192.168.140.180
Ei liikennettä muiden laitteiden, kuin 192.168.140.178-179 kanssa.

192.168.140.181
Laitteen liikenne koostuu ainoastaan oman aliverkon ulkopuolelle lähetetyistä NTP-paketeista.

192.168.140.200
Suurin osa liikenteestä lähetettyjä ja vastaanotettuja UDP-paketteja.

192.168.140.201
Ainoastaan UDP-liikennettä.

192.168.140.202
Ainoastaan UDP-liikennettä.

192.168.140.254
Wireshark-kuuntelun aikana ei kaapattu ainuttakaan pakettia.

5. YHTEENVETO

Harjoitusten aikana verkosta löydettiin valtavat määrät satunnaista tietoa, joka ei pohjatiedot huomioiden aluksi juurikaan hetkauttanut lukijaa. Raporttia tuottaessa koko liikenne käytiin läpi uudelleen, jolloin osa asioista selkeytyi ja merkitys korostui.

Etenkin Zenmap ja Nessus olivat esimerkiksi joidenkin laitteiden käyttöjärjestelmistä eri mieltä. Ongelma selittynee sillä, että Zenmapin analyysin mukaan esimerkiksi laitteen IP: 192.168.140.200 käyttöjärjestelmä oli

OS details: Microsoft Windows Server 2008 SP2, Microsoft Windows 7 SP0 – SP1, Microsoft Windows Server 2008 SP1, or Windows 8

, joista se luultavasti arpoi ensimmäisen vaihtoehdon oikeaksi. Nessuksen mukaan käyttöjärjestelmä oli Microsoft Windows 7 Enterprise, varmuudella 99.

Verkon analysointi oli tehtävänannosta johtuen jokseenkin haasteellista, eikä harjoituksissa varsinaisesti annettu eväitä sen tekemiseen. Mikäli harjoituksien ainoana tavoitteena oli käytettyihin työkaluihin yleisellä tasolla tutustuminen, päästiin tavoitteeseen varmasti hyvin kaikkien osalta. Syväluotaavampi opastaminen harjoituksissa on kuitenkin tarpeen, jos tarkoituksena on ymmärtää edes yleisesti mitä tapahtuu ja miksi näin tehdään.

Vasta harjoitustyöohjeesta löytyi selkeästi eriteltynä asiat ja tiedot, mitä verkosta olisi pitänyt harjoitusten aikana selvittää!

Tästä syystä koko liikenne jouduttiin tarkemman alayysin yhteydessä käymään alusta asti uudelleen. Harjoituksen aihepiiri kuitenkin herätti mielenkiinnon ja vastaavia toivottavasti tulee lisää.

LÄHTEET

[1] Nmap, Wikipedia, viitattu 15.12.2015. Saatavissa: https://en.wikipedia.org/wiki/Nmap

[2] Zenmap, nmap.org. Viitattu 15.12.2015. Saatavissa: https://nmap.org/zenmap/

[3] Nessus, Wikipedia, viitattu 15.12.2015. Saatavissa: https://en.wikipedia.org/wiki/Nessus_(software)

[4] Top 125 Network Security Tools, SecTools, viitattu 15.12.2015. Saatavissa: http://sectools.org/

[5] Nessus, Tenable Network Security, viitattu 15.12.2015. Saatavissa: http://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/images/product-images/agent-dashboard-no-frame.png

[6] Wireshark, Wikipedia, viitattu 16.12.2015. Saatavissa: https://en.wikipedia.org/wiki/Wireshark

[7] Zenmap GUI Users' Guide, nmap.org, viitattu 16.12.2015. Saatavissa: https://nmap.org/book/zenmap-topology.html