jamk

Labra 3

Ryhmä 3

Antti Tammelin

Tero Räsänen

Elmeri Söderholm

Eliel Taskinen

Raportti

Syyskuu 2022

Tieto- ja viestintätekniikan tutkinto-ohjelma

Tietoturvakontrollit TTC6010-3002

3.10.2022

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

1 Johdanto

Labra 3 on Tietoturvakontrollit TTC6010-3002 kurssin ryhmätyö. Labra 3:ssa tutkimme tarkemmin Paloalton turvallisuusominaisuuksia. Aiheena on tässä labrassa Paloalton Threat-ID:n sekä URL filteröinnin käyttö.

1.1 Tehtävänanto

Labran tehtävänantona oli lisätä palomuuriin sääntö, joka lisäsi Antiviruksen, vulnerability protectionin, anti-spywaren, file blockingin, sekä Wildfire analysisin DMZ:stä VLE:hen kulkevaan liikenteeseen. Tämän teimme valmiiksi, ja dokumentoimme, mutta selitämme mitä eri asetukset tekivät teoreettisesti. Sen lisäksi palomuuriin piti lisätä WS-Netistä VLE:hen sääntö, mikä teki monia samanlaisia asioita kuin DMZ to VLE palomuurisääntö (Lab 3 ohjeet. N.d.).

WS-Netistä VLE:hen sääntö, tai tästä lähtien WS-TO-VLE, koostui uudesta antivirusprofiilista, mikä hälytti kaikista mahdollisista lähteistä eikä yrittänyt esimerkiksi estää tiedoston lataamista, URL-filtteröinnistä, missä yle.fi on blokattu, uhkapelisivustot aiheuttavat hälytyksen, ja games sivustoihin pääsee continue vaihtoehdolla. Näiden lisäksi eicar.com tai eicar.org sivustolta ladattavan testitiedoston piti osua tehtyyn antivirusprofiiliin, ja hälyttää palomuurin sisällä (Lab 3 ohjeet. N.d.).

Näiden kahden tehtävän lisäksi labrassa oli ekstratehtävä, flood protection. Tehtävänantona tässä oli estää tai edes alerttaa skannaukset Admine-Netissä olevasta Kali-linux virtuaalisesta koneesta DMZ:lla olevalle www-koneelle. Kokeilimme suorittaa tämänkin, ja olemme dokumentoineet sen erikseen (Lab 3 ohjeet. N.d.).

1.2 Labrassa käytetyn ympäristön kuvaus

Kolmas labra keskittyi pääsääntöisesti VLE:n palomuuriin, jota konfiguroitiin erilaisilla säännöillä. Jotta me pystyisimme testaamaan näitä labran aikana tehtyjä sääntöjä, käytimme muita osia

VLE:stä. WS-TO-VLE:n testaamisen käytimme WS-Netissä ollutta ainoaa konetta WS01, josta yritimme saada yhteyden internettiin. Sen lisäksi flood protectionin aikana tarvitsimme Admin-Netistä Kali virtuaalista konetta, ja DMZ:sta www virtuaalista konetta (ks. liite 1).

2 Teoria

Tämän raportin teoriaosuudessa käymme läpi termit Kali Linux, Nmap, Threat ID (Threat Vault), URL-filtering sekä https decryption.

2.1 Kali Linux

Kali Linux on ilmainen avoimen lähdekoodin Debian-Linux pohjainen käyttöjärjestelmä. Kali Linux on tarkoitettu edistyneeseen penetraatiotestaukseen ja tietoturvatarkastukseen. Se sisältää satoja työkaluja, jotka on suunnattu erilaisiin tietoturvatehtäviin, esim. forensiikkaan, takaisin mallintaminen, red team testaukseen ja moniin muihin samanlaisiin tehtäviin (What is Kali Linux? 2022).

2.2 Nmap

Nmap (“Network Mapper”) on ilmainen ja avoimen lähdekoodin ohjelma verkon skannaukseen ja tietoturvatarkastukseen. Nmap käyttää raaka-IP-paketteja uusilla tavoilla määrittääkseen, mitkä hostit ovat saatavilla verkossa, mitä palveluita (sovelluksen nimi ja versio) kyseiset hostit tarjoavat, mitä käyttöjärjestelmiä (ja käyttöjärjestelmäversioita) ne käyttävät, minkä tyyppiset pakettisuodattimet/palomuurit ovat käytössä ja kymmeniä muita ominaisuuksia. Se on suunniteltu skannaamaan nopeasti suuria verkkoja, mutta se toimii hyvin myös yksittäisiä isäntiä vastaan. Nmap on Kali-Linuxissa valmiiksi asennettuna (Nmap: Discover your network. N.d.).

2.3 Threat ID

Threat ID on termi, jota käytetään Palo Alton uhkien etsinnässä. Uhkia pystyy etsimään Palo Alton Threat Vaultissa, joka on siis erillinen tietokanta, josta voi hakea ja tutkia erilaisia uhkia. Threat ID

on haetun uhkan uniikki signeeraus, joka kertoo uusimmat tiedot uhkasta mitä Palo Altolla on tarjota. Tiedot voivat sisältää mm. ensimmäisen ja viimeisen sisältöjulkaisun päivityksiä varten (Threat Details N.d.).

2.4 URL Filtering

URL-filteringin (URL-suodatus) avulla verkon liikennettä suodatetaan palomuurista löytyvän tietokannan mukaan. Yleisin syy URL-suodatukseen on ollut estää pääsy työajalla nettisivuille, jotka eivät liity työntekoon, esimerkiksi Facebookiin tai Instagramiin. Nykyään voidaan estää pääsy myös kategorian perusteella ilman tiettyä nettiosoitetta. Silloin pääsy kaikille tietyn tyyppisille sivuille estetään. Pelkkä URL-suodatus on usein riittämätön suojaus, koska sen avulla ei pystytä riittävästi suojaamaan verkkoliikennettä tai estämään haittaohjelmia. Lisäksi kannattaa käyttää palomuurin muita ominaisuuksia suodatuksen lisäksi. (What is URL Filtering? 2022.)

2.5 https Decryption

Https-lyhenteen viimeinen kirjain s tulee sanasta SSL/TLS-protocol. Se salaa kaiken käyttäjän ja nettisivun välisen liikenteen. Suojatuilla sivuilla on turvallista tehdä verkko-ostoksia tai kirjautua sähköiseen palveluun. Valitettavasti salattu yhteys on myös mahdollisuus hyökkääjälle piilottaa salatun liikenteen sekaan omaa, haitallista liikennettä. Tämän takia tarvitaan https decryptionia, suomeksi siis https salauksen purkua. Samaa asiaa tarkoittaa SSL-liikenteen purku (Decrypt or Die! 2017).

Yleisimpiä syitä salauksen purulle on uuden sukupolven palomuurien (kuten Palo Alto) tietoturvaominaisuuksien tehokkaampi käyttö. Haittaohjelmien suodatus- sekä hyökkäystenestomenetelmät toimivat tehokkaammin, jos niitä voi käyttää myös salattuun liikenteeseen (Decrypt or Die! 2017).

Jos salauksen purku otetaan käyttöön, kannattaa miettiä mihin sitä käytetään. Firman koko nettiliikenteen salauksen purkamisessa ei ole järkeä, ja se söisi resursseja muista suojaustoimenpiteistä. Siksi purku kannattaa keskittää korkeamman riskitason kohteisiin. Lisäksi esimerkiksi pankkien tai

sairaaloiden verkkoliikenne pitää jättää purkamatta, koska se ei olisi edes laillista. Jotta salauksen purku voidaan ottaa firmassa käyttöön, pitää ensin käydä YT-neuvottelut, jossa henkilöstölle kerrotaan tarkemmin purusta ja siitä, miten se tapahtuu (Decrypt or Die! 2017).

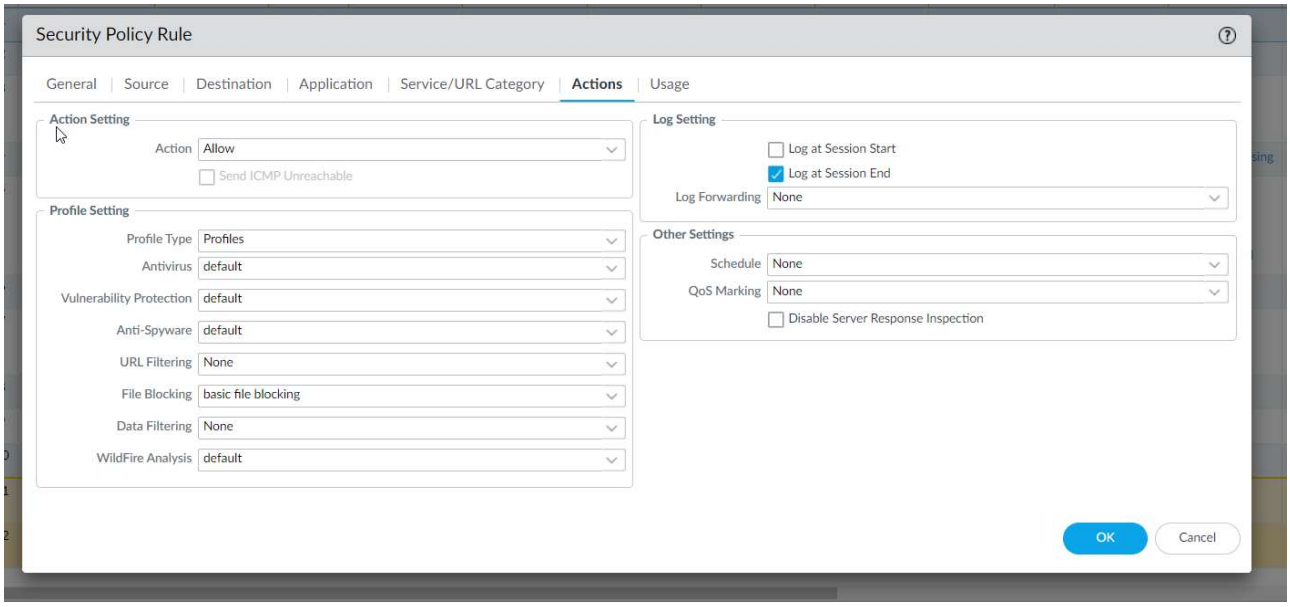
3 DMZ filtteröity yhteys VLE:hen

Ensimmäisenä tehtävänä oli filtteröidä DMZ:n ja VLE:n välistä liikennettä, ja lisätä siihen tarvittavat turvallisuuspolitiikkaprofiilit, mitä tehtävänannossa pyydetään. Poistimme tämän liikenteen muista palomuurin säännöistä, ja lisäsimme palomuurin `**Policies**` kohtaan `**Security**` uuden säännön tälle DMZ:sta VLE:hen kulkevaan liikenteeseen (ks. kuvio 1).

				Source				Destination					
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
1	DMZ-TO-VLE	none	universal	DMZ	any	any	any	VLE	any	any	any	application-...	Allow

Kuvio 1. DMZ-TO-VLE palomuurisääntö.

Tehtävänannossa piti myös laittaa tähän uuteen sääntöön Antivirus, anti-spyware, file blocking, sekä wildfire analysis päälle default/basic muodossa. Näihin profiileihin ei pitänyt konfiguroida paljoa, vaan ne löytyivät, kun klikkasi muokattavaa sääntöä, josta aukeaa `**Security Policy Rule**`. `**Actions**` kohdan alta löytyy profiilit, josta pystyi valitsemaan kaikki tarvittavat profiilit (ks. kuvio 2).



Kuvio 2. Security Policy Rule Profiilit.

Nyt commitin jälkeen pitäisi kaikkien näiden toimia, mutta emme pystyneen kokeilemaan tätä enempää, ja opettajan mukaan sitä ei tarvinnut testata. Sen sijasta selitämme, mitä eri profiilit tekisivät teoreettisesti, ja minkä takia eri profiilit ovat olemassa.

3.1 Eri turvallisuuspolitiikkaprofiilit

3.1.1 Antivirus

Antivirus tai toiselta nimeltään virustorjunta, on ohjelma palomuurissa, jota käytetään haittaohjelmien havaitsemiseen, estämiseen ja poistamiseen. Paloalton antivirus tunnistaa hyvin paljon erityyppisiä haitallisia ohjelmia ja tekee sen niin, ettei palomuurin suorituskyky heikkene merkittävästi (Security Profiles. N.d).

3.1.2 Vulnerability Protection

Vulnerability Protection on ominaisuus Palo Alton turvallisuuspolitiikassa, jolla voi määrittää sopiva turvallisuustaso laittomia koodauksia ja muita yrityksiä varten, joilla yritetään käyttää hyväksi

järjestelmän haavoittuvuuksia. Paloaltossa on kaksi ennakkoon määritettyä asetusta. Oletusasetus eli default havaitsee korkean ja keskitason haavoittuvuudet, mutta ei matalan tason haavoittuvuuksia. Tiukka asetus havaitsee kaikki haavoittuvuudet ja käyttää erillistä oletusasetusta havaitakseen matalan tason sekä myös pelkästään tiedottavia haavoittuvuuksia (Security Profiles N.d).

3.1.3 Anti-spyware

Anti-spyware on turvallisuusprofiili, jolla pystyy estämään vaarantuneita käyttäjiä lähettämästä tietoa ulkopuolelle, Anti-spywaren avulla pystyy samalla havaitsemaan uhkaavaa lähtevää liikennettä verkon tartutetuista asiakkaista. Tätä profiilia pystyy myös säätämään Paloaltossa erilaisilla säännöillä. Näitä on Default, Allow, Alert, Drop, Reset Client, Reset Server Reset Both ja Block IP (Security Profiles N.d).

3.1.4 File Blocking

File Blocking-toiminnon avulla voidaan estää tai tarkkailla tietyn tyyppisiä tiedostoja. Tiedostot voidaan eritellä joko tiedoston päätteen tai tiedoston tyypin mukaan. File Blocking vaihtoehtoja on monia mitä tiedostolle pystytään tekemään. Tiedostot pystytään estämään, tai niiden lataus voidaan sallia, mutta koneen käyttäjää huomautetaan tästä latauksesta, tai tiedoston lataus hälyttää ilman käyttäjän tietämättä tarpeellisille tahoille. Palo Alto-palomuureissa on valmiina kaksi file blocking-profiilia, joita käytetään sen mukaan kuinka haavoittuvasta ohjelmasta, on kyse, basic ja strict. Näitä profiileja voi muokata, mutta sitä ei suositella kuin välttämättömissä tapauksissa, jotta tietoturva ei kärsi (Set Up File Blocking. 2022).

3.1.5 Wildfire analysis

Wildfire on Palo Alton tietokanta, johon Palo Alton palomuurit lähettää tiedot jokaisesta käyttäjän koneella havaitusta zero-day haavoittuvuudesta. Kaikki Palo Alto käyttäjät ovat yhteydessä tähän tietokantaan. Wildfiren avulla kaikki Palo Alto-palomuurit saavat reaaliajassa tiedot liikkeellä olevista haittaohjelmista. Näin yksittäisen palomuurin havaitsema haittaohjelma saadaan torjuttua kaikissa Palo Alto-palomuureissa ympäri maailman viiden minuutin sisällä (About WildFire. 2022).

4 WS-Netistä yhteys VLE:hen

WS-TO-VLE säännössä oli paljon enemmän tekemistä kuin DMZ-TO-VLE säännössä. Seurasimme pitkälle ohjeissa ollutta järjestystä, joten selitämme myös kaiken samassa järjestyksessä (Lab 3 ohjeet. N.d.).

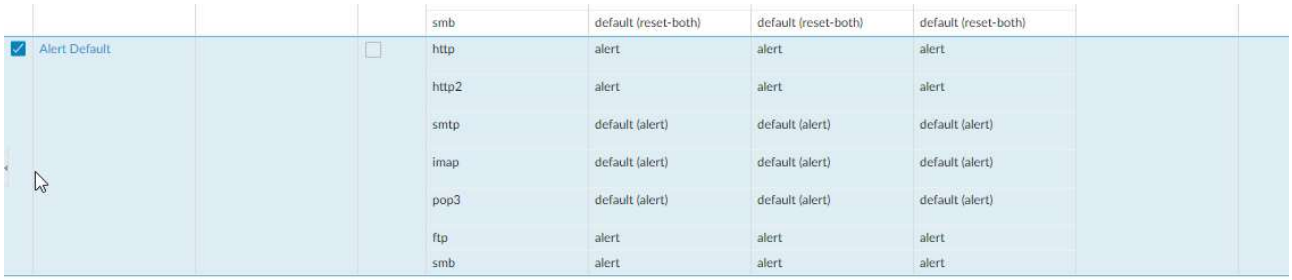
4.1 Antivirus profiili

Ensin aloimme tekemään tehtävänannossa kuvailtua Antivirus profiilia. Default Antivirus profiilissa oli sekoitus alertteja ja reset-both asetuksia (ks. kuvio 3).

NAME	LOCATION	PACKET CAPTURE	PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
default	Predefined		http	default (reset-both)	default (reset-both)	default (reset-both)
			http2	default (reset-both)	default (reset-both)	default (reset-both)
			smtp	default (alert)	default (alert)	default (alert)
			imap	default (alert)	default (alert)	default (alert)
			pop3	default (alert)	default (alert)	default (alert)
			ftp	default (reset-both)	default (reset-both)	default (reset-both)
			smb	default (reset-both)	default (reset-both)	default (reset-both)
Lab3_Antivirus_Profile			http	alert	alert	alert

Kuvio 3. default settings.

Uuteen Antivirus profiiliin, mikä aluksi kopioitiin default profiilista, joten siinä oli kaikki samat asetukset, piti asettaa kaikki kohdat alerttiin (ks. kuvio 4).



	smb	default (reset-both)	default (reset-both)	default (reset-both)
Alert Default	http	alert	alert	alert
	http2	alert	alert	alert
	smtp	default (alert)	default (alert)	default (alert)
	imap	default (alert)	default (alert)	default (alert)
	pop3	default (alert)	default (alert)	default (alert)
	ftp	alert	alert	alert
	smb	alert	alert	alert

Kuvio 4. Antivirus Security Profile hälytykset.

4.2 URL Filttering

Kun Antivirus profiili on tehty, aloimme tekemään URL filtteröintiä. URL filtteröinnissä piti ”Gambling” tai uhkapelisivustot tehdä hälytyksen ja ”Games” sivustoihin pystyisi päästä normaalisti ”continue” vaihtoehdolla. Continue asetus antaa mennä sivustolle, mutta ensin se varoittaa, että tälle sivulle meneminen aiheuttaa alertin palomuurissa. Sen lisäksi piti tehdä kahdelle sivustolle mukautetut URL kategoriat, yle.fi ja eicar.com tai eicar.org. Pystyimme tekemään mukautetut URL-kategoriat `**Objects**` alta `**Custom Objects**` kohdasta `**URL Category**` alta, josta teimme kummallekin, yle ja eicar sivustoille, omat objektit. Objekteissa on kaikki mahdolliset sivut mitä sivustojen alla on (ks. kuvio 5).

NAME	LOCATION	TYPE	MATCH
Yle		URL List	yle.fi
			*.yle.fi
eicar		URL List	eicar.com
			*.eicar.com
			eicar.org
			*.eicar.org

Kuvio 5. Url Objektit yle ja eicar.

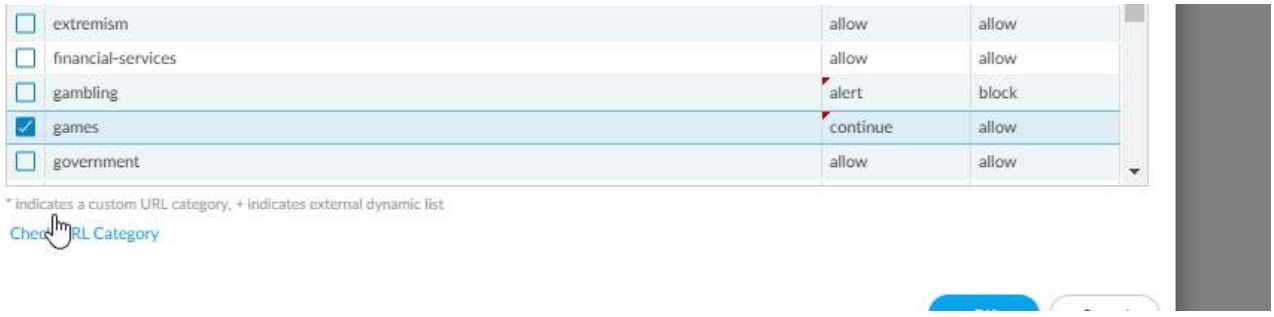
Sen jälkeen pystyimme lisäämään nämä säännöt, normaaleille URL kategorioille ja mukautetuille URL kategorioille, URL filtering profiiliin `**Objektien**` `**Security Profiles**` kohdasta, josta löytyy `**Url**

Filtering`. Teimme saman asian kuin mitä Antiviruksen kanssa, eli kopioimme default profiilin, ja teimme sen päälle muutoksia (ks. kuvio 6).

NAME	LOCATION	SITE ACCESS	USER CREDENTIAL SUBMISSION	HTTP HEADER INSERTION	INLINE ML
default	Predefined	Allow Categories (58) Alert Categories (5) Continue Categories (0) Block Categories (11) Override Categories (0)	Allow Categories (74) Alert Categories (0) Continue Categories (0) Block Categories (0)		Allow Categories (0) Alert Categories (1) Block Categories (1)
Lab3_URL_Filtt...		Allow Categories (59) Alert Categories (6) Continue Categories (1) Block Categories (10) Override Categories (0)	Allow Categories (64) Alert Categories (0) Continue Categories (0) Block Categories (11)		Allow Categories (0) Alert Categories (1) Block Categories (1)

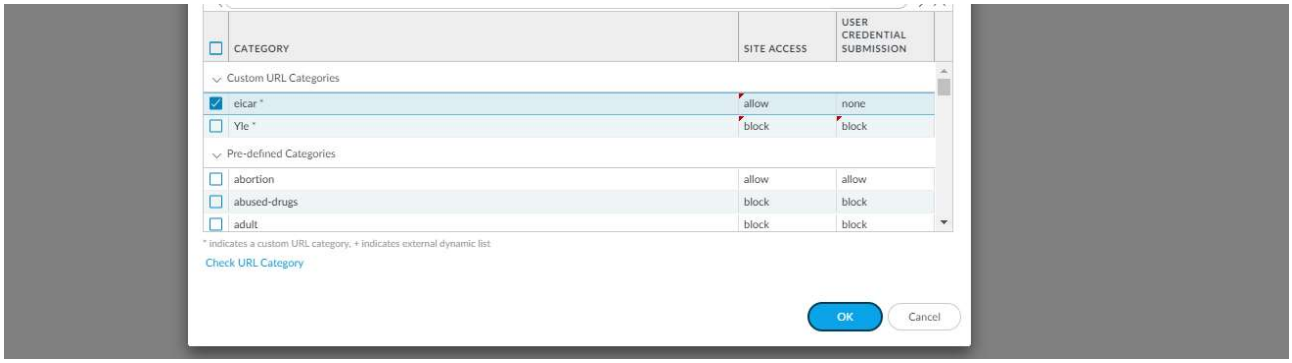
Kuvio 6. Kopioitu URL Filttering profiili.

Vaihdoimme vain muutamasta kohdasta asetuksia Url Filtering profiilissa. Games kohdalle laitoimme Continue vaihtoehdon, ja Gambling kohtaan alertin (ks. kuvio 7).



Kuvio 7. URL filtterit pelit ja uhkapelisivustot.

Saman profiilin asetuksista lisäsimme mukautetut URL kategoriat, ja asetimme niille säännöt oikein. Yle.fi piti kokonaan blokata, ja eicar yllättävästi sallittiin kokonaan menemään läpi (ks. kuvio 6).



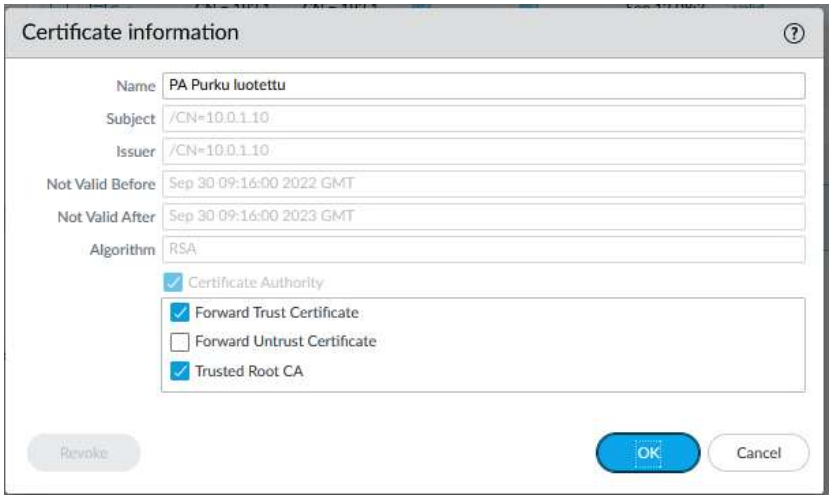
Kuvio 8. URL filtterit custom url kategoriat.

Eicar päästettiin kokonaan läpi, mutta se pitää kuitenkin olla säännöissä, jotta voimme tehdä seuraavat vaiheet, esimerkiksi https decryption, oikein.

4.3 https decryption

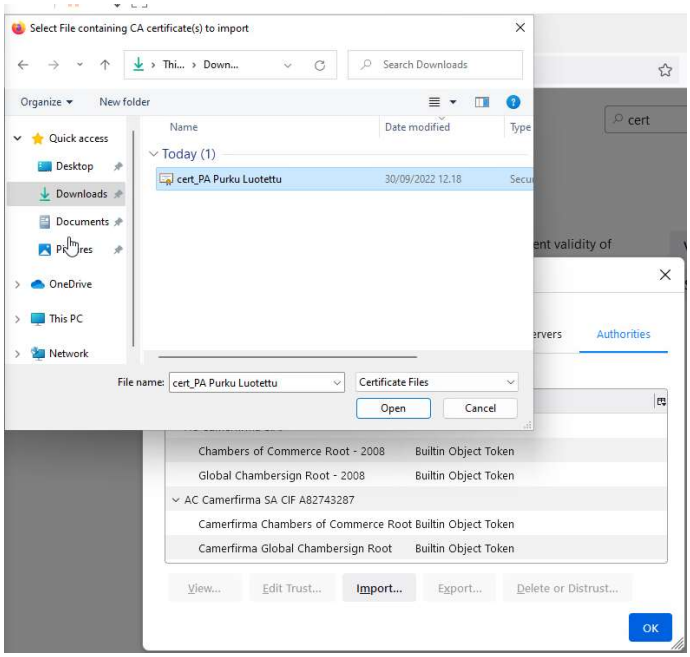
Jos nyt menisimme yle.fi sivuille, pääsisimme sivustolle ilman mitään ongelmia, vaikka sääntöjen mukaan meidän ei pitäisi päästä sivustolle. Tämä johtuu, että yhteys on enckryptattu, eli yhteys on https eikä http. Enkryptauksen takia palomuuri ei näe sivustoja, joten palomuuri ei pysty blokkaamaan sivustoja. Sen takia meidän pitää dekryptata https. https:än dekryptauksesta kirjoitimme enemmän teoriaosuudessa.

Palomuurin sisällä ensin tehdään sertifikaatti, mikä onnistuu `**Device**` kohdalta `**Certificate Management**` alta kohdasta `**Certificates**`. Palo Alton interfacessa on alhaalla nappi generate, jolla pystyy generoimaan uuden sertifikaatin. Nimesimme sertifikaatin PA Purku luotettu, ja certifikaattiin piti laittaa `**Forward Trust Certificate**` ja `**Trusted Root CA**` jotta https decryption onnistuisi (ks. kuvio 9).



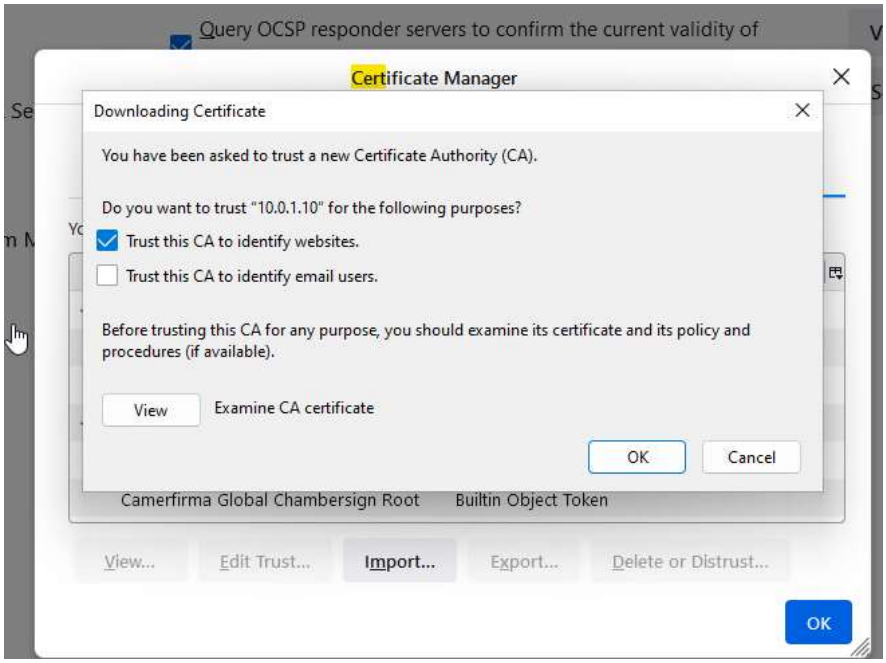
Kuvio 9. https purku cert luotu.

Kun sertifikaatti on tehty, avasimme palomuurin interfacen browserin kautta WS01 virtuaalisessa koneessa, josta latasimme äsken tehdyn sertifikaatin WS01:lle. Sen jälkeen lisäsimme sen Firefoxin luotettuihin sertifikaatteihin (ks. kuvio 10).



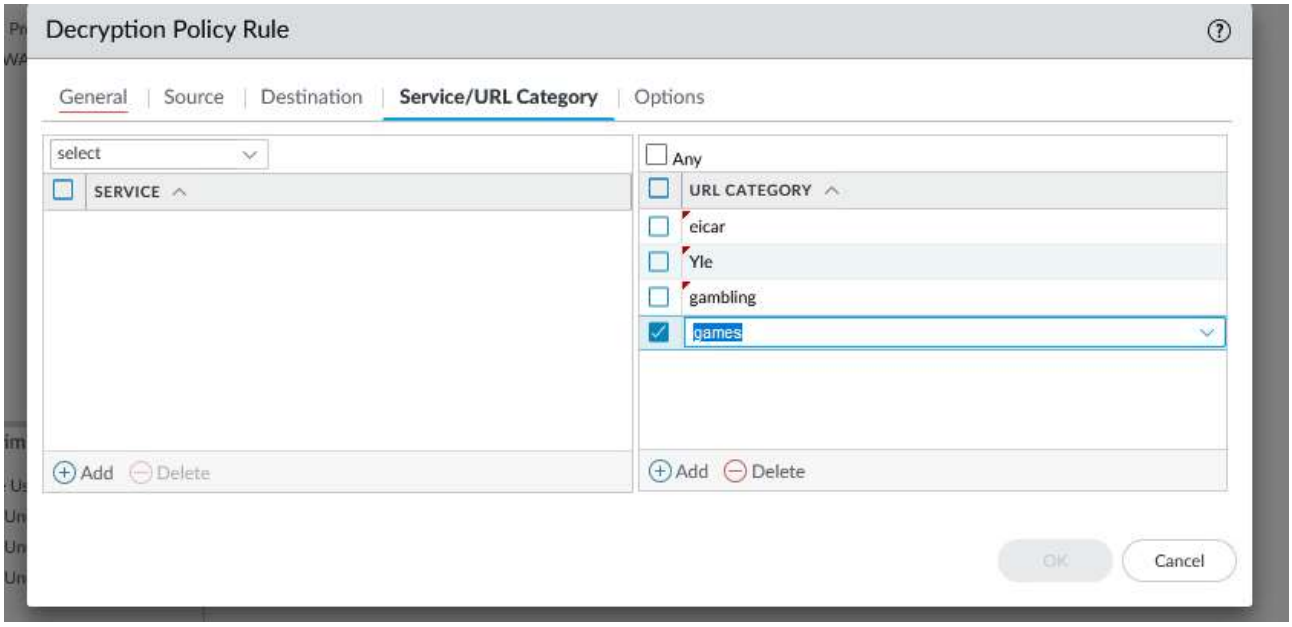
Kuvio 10. HTTPS purun CA lisätty firefoxiin.

Sertifikaatin importtaamisessa Firefoxiin piti myös laittaa `**Trust this CA to identify websites.** ` valinta päälle (ks. kuvio 11).



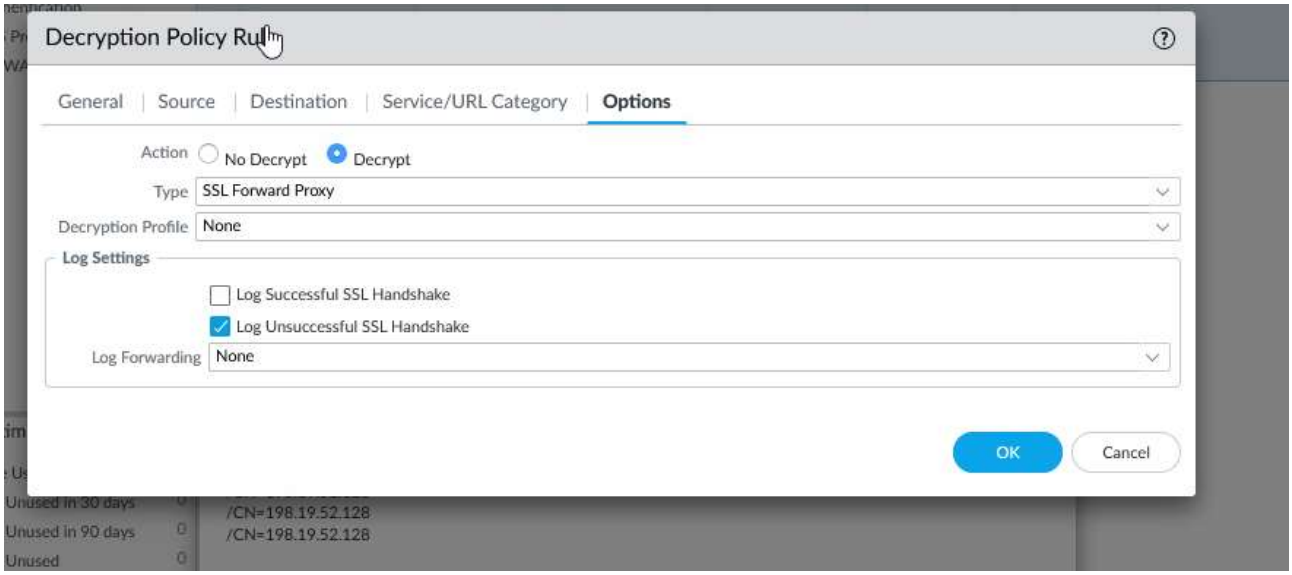
Kuvio 11. Firefox asetukset.

Kun sertifikaatti on lisätty Firefoxiin, pitää palomuurin sisällä tehdä decrypting sääntö, joka määrittelee mistä sourcesta ja mihin destinationiin liikenne mikä dekryptataa voi mennä, ja mihin URL kategorioihin dekryptaus toimii. Dekryptaus löytyy `**Policies**` alta `**Decryption**` kohdasta. Palomuurin interfacesta alhaalta pystyy lisäämään uuden säännön. Dekryptauksen source oli WS-NET, ja destination VLE, samalla tavalla kuin WS-TO-VLE palomuurin security säännössä. URL kategorioiksi laitoimme kaikki, mitä olemme käyttäneet aiemmin labrassa, eli gambling ja games normaaleista URL kategorioista, ja yle ja eicar mukautetuista URL kategorioista (ks. kuvio 12).



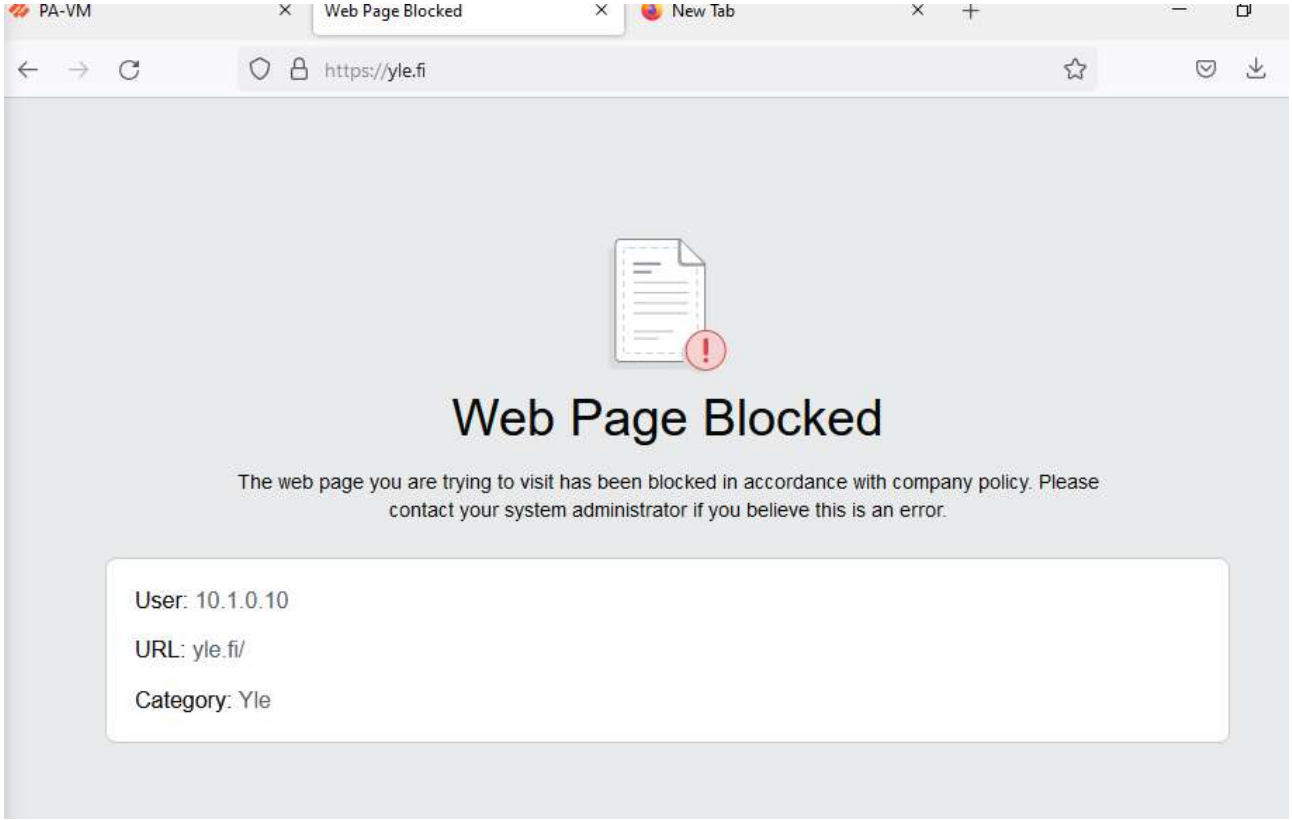
Kuvio 12. Decryption Policyt.

URL kategorioiden lisäksi piti konfiguroida dekryptauksen `**Options**` kohdasta kuvan mukaiseksi, pääosin Decrypt päälle, ja varmistaa että SSL Forward Proxy on päällä (ks. kuvio 13).



Kuvio 13. Decryption policyt options.

Näiden asetusten jälkeen pitäisi nyt sääntöjen toimia kunnolla. Kokeilimme kaikkia eri sääntöjä mitä meidän piti konfiguroida, joista esimerkkinä yle.fi osoitteen blokkaaminen (ks. kuvio 14).



Kuvio 14. yle.fi blokattu

Otimme myös muista kategorioille, gambling ja games, tehdyille säännöille lokitiedostojen muodossa. Lokeista huomaa, miten gambling kategoria hälyttää, ja games sivuilla on continue vaihtoehto (ks. kuvio 15).

RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	APPLICATION	ACTION	HEADERS INSERTED	HTTP/2 CONNECTION SESSION ID
09/30 12:29:06	gambling	gambling,low-risk	www.unibet.com/	WS-NET	VLE	10.1.0.10			85.184.96.0			web-browsing	alert		40938
09/30 12:29:06	gambling	gambling,low-risk	www.unibet.com/	WS-NET	VLE	10.1.0.10			85.184.96.0			web-browsing	alert		40938
09/30 12:28:51	games	games,low-risk	workers.crazyga...	WS-NET	VLE	10.1.0.10			104.17.196.57			web-browsing	continue		41366
09/30 12:28:46	games	games,low-risk	images.crazygam...	WS-NET	VLE	10.1.0.10			151.101.246.208			web-browsing	continue		41191
09/30 12:28:46	games	games,low-risk	builds.crazygam...	WS-NET	VLE	10.1.0.10			104.17.196.57			web-browsing	continue		41206
09/30 12:28:46	games	games,low-risk	builds.crazygam...	WS-NET	VLE	10.1.0.10			104.17.196.57			web-browsing	continue		41206
09/30 12:28:46	games	games,low-risk	builds.crazygam...	WS-NET	VLE	10.1.0.10			104.17.196.57			web-browsing	continue		41206
09/30 12:28:46	games	games,low-risk	builds.crazygam...	WS-NET	VLE	10.1.0.10			104.17.196.57			web-browsing	continue		41206
09/30 12:28:46	games	games,low-risk	builds.crazygam...	WS-NET	VLE	10.1.0.10			104.17.196.57			web-browsing	continue		41206
09/30 12:28:46	games	games,low-risk	builds.crazygam...	WS-NET	VLE	10.1.0.10			104.17.196.57			web-browsing	continue		41206
09/30 12:28:46	games	games,low-risk	www.crazygame...	WS-NET	VLE	10.1.0.10			104.17.196.57			web-browsing	continue		41206
09/30 12:28:46	games	games,low-risk	images.crazygam...	WS-NET	VLE	10.1.0.10			151.101.246.208			web-browsing	continue		41191
09/30 12:28:46	games	games,low-risk	images.crazygam...	WS-NET	VLE	10.1.0.10			151.101.246.208			web-browsing	continue		41191
09/30 12:28:46	games	games,low-risk	builds.crazygam...	WS-NET	VLE	10.1.0.10			104.17.196.57			web-browsing	continue		41206

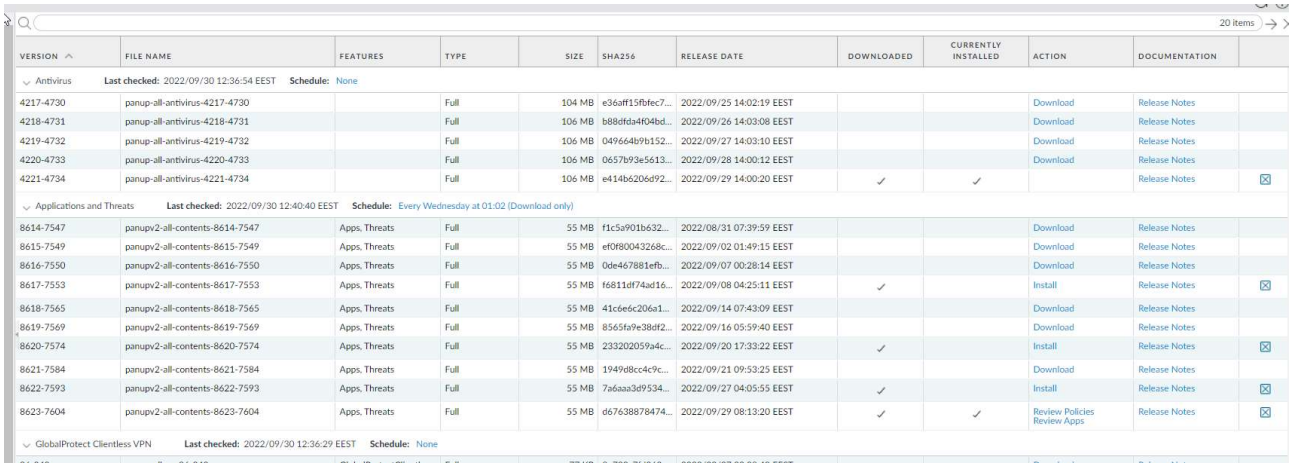
Kuvio 15. Gambling alert, games continue.

Näistä kuitenkin puuttui yksi URL kategoria, eicar. Tätä varten pitää jatkaa konfigurointia.

4.4 Eicar, testitiedoston hälyttäminen

Tällä hetkellä eicar URL kategoria toimii sääntöjen mukaan, ja siinä toimii https dekryptaus. Kuitenkin tämä ei ole täysin mitä me haluamme sen tekevän. Labrassa kun eicar sivustolta lataa tiedoston, sen pitäisi osua tehtyyn antivirusprofiiliin, ja hälyttää palomuurin sisällä, että epäilyttävä tiedosto on ladattu.

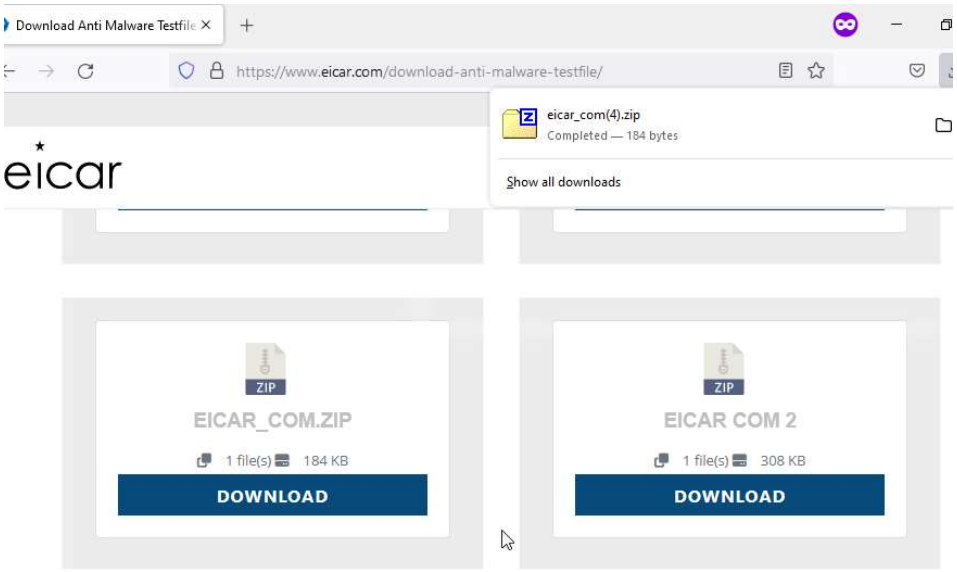
Olimme tehneet jo profiilin antivirukselle, joten seuraava askel oli ladata tarvittavat tiedostot antiviruksen toimintaan palomuurin sisälle. ne löytyvät `**Device**` kohdasta `**Dynamic Updates**`. Tämän valikon alakulmasta löytyy `**Check Now**`, joka tarkistaa ja antaa vaihtoehdoksi uusimman päivityksen antivirukselle ja muihin profiileihin. Latasimme ja asensimme uusimmat paketit kohdista `**Antivirus**` ja `**Applications and Threats**` (ks. kuvio 16).



VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION	DOCUMENTATION
Antivirus	Last checked: 2022/09/30 12:36:54 EEST	Schedule: None								
4217-4730	panup-all-antivirus-4217-4730		Full	104 MB	e36aff15fbfec7...	2022/09/25 14:02:19 EEST			Download	Release Notes
4218-4731	panup-all-antivirus-4218-4731		Full	106 MB	b88dfda4f04bd...	2022/09/26 14:03:08 EEST			Download	Release Notes
4219-4732	panup-all-antivirus-4219-4732		Full	106 MB	049664b9b152...	2022/09/27 14:03:10 EEST			Download	Release Notes
4220-4733	panup-all-antivirus-4220-4733		Full	106 MB	0657b93e5613...	2022/09/28 14:00:12 EEST			Download	Release Notes
4221-4734	panup-all-antivirus-4221-4734		Full	106 MB	e414b6206d92...	2022/09/29 14:00:20 EEST	✓	✓		Release Notes
Applications and Threats	Last checked: 2022/09/30 12:40:40 EEST	Schedule: Every Wednesday at 01:02 (Download only)								
8614-7547	panupv2-all-contents-8614-7547	Apps, Threats	Full	55 MB	f1c5a901b632...	2022/08/31 07:39:59 EEST			Download	Release Notes
8615-7549	panupv2-all-contents-8615-7549	Apps, Threats	Full	55 MB	ef0f80043268c...	2022/09/02 01:49:15 EEST			Download	Release Notes
8616-7550	panupv2-all-contents-8616-7550	Apps, Threats	Full	55 MB	0de467881efb...	2022/09/07 00:28:14 EEST			Download	Release Notes
8617-7553	panupv2-all-contents-8617-7553	Apps, Threats	Full	55 MB	f6811df74ad16...	2022/09/08 04:25:11 EEST	✓		Install	Release Notes
8618-7565	panupv2-all-contents-8618-7565	Apps, Threats	Full	55 MB	41c6e6c206a1...	2022/09/14 07:43:09 EEST			Download	Release Notes
8619-7569	panupv2-all-contents-8619-7569	Apps, Threats	Full	55 MB	8565fa9e38df2...	2022/09/16 05:59:40 EEST			Download	Release Notes
8620-7574	panupv2-all-contents-8620-7574	Apps, Threats	Full	55 MB	233202059a4c...	2022/09/20 17:33:22 EEST	✓		Install	Release Notes
8621-7584	panupv2-all-contents-8621-7584	Apps, Threats	Full	55 MB	1949d8cc4c9c...	2022/09/21 09:53:25 EEST			Download	Release Notes
8622-7593	panupv2-all-contents-8622-7593	Apps, Threats	Full	55 MB	7a6aaa3d9534...	2022/09/27 04:05:55 EEST	✓		Install	Release Notes
8623-7604	panupv2-all-contents-8623-7604	Apps, Threats	Full	55 MB	d6763887847 4...	2022/09/29 08:13:20 EEST	✓	✓	Review Policies Review Apps	Release Notes
GlobalProtect Clientless VPN	Last checked: 2022/09/30 12:36:29 EEST	Schedule: None								

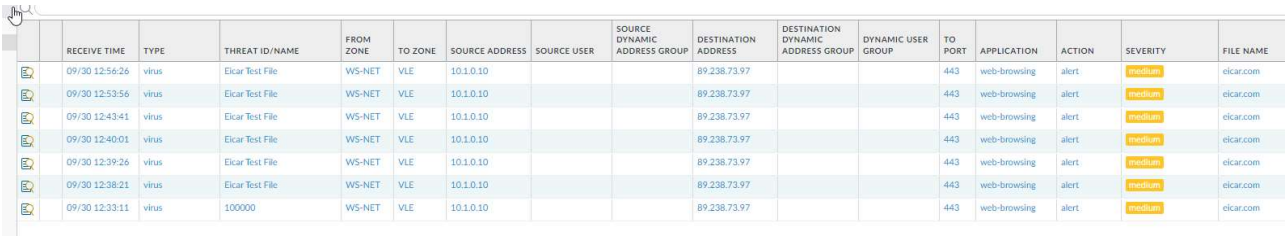
Kuvio 16. antivirus, ja threats and applications asentaminen palomuuriin.

Näiden jälkeen pitäisi antivirusprofiilin toimia ohjeiden mukaan. Latasimme eicar sivustolta kokeilutiedoston `**eicar_com.zip**` (ks. kuvio 17).



Kuvio 17. Ladattu testitiedosto antivirukselle.

Meillä oli hiukan ongelmia tämän vaiheen kanssa, koska opettajan näyttämässä videossa tuli erilainen lopputulos, joka oli myöskin paljon selkeämpi ja näkyvämpi lopputulos kuin mikä meidän lopputuloksemme oli. Opettajan näyttämässä videossa tiedoston lataus kokonaan estettiin, mutta meidän ohjeiden mukainen profiili pelkästään teki alertin palomuurin sisälle, että tiedosto oli ladattu. Kuitenkin saimme hälytykset näkymään, kun tajusimme tarkistaa `**Monitor**` kohdan alta `**Threats**` kohdasta, ja näimme tiedoston tekemät hälytykset (ks. kuvio 16).

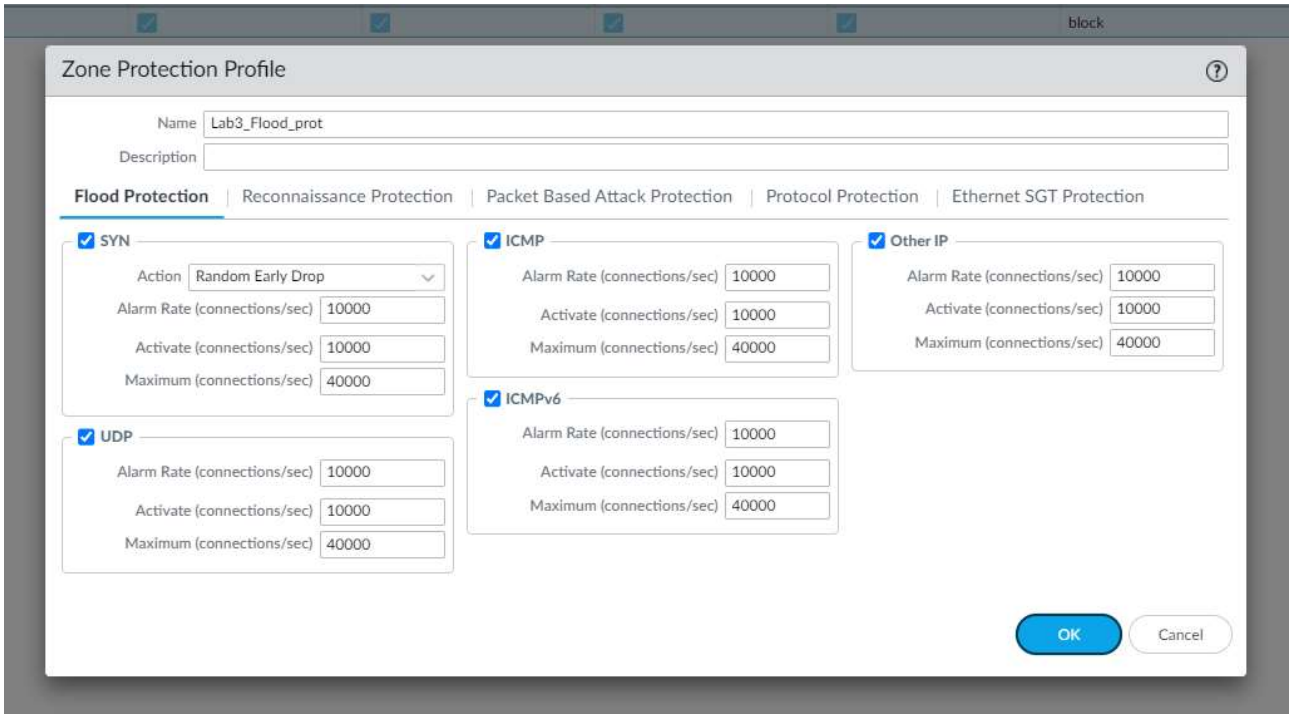


	RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	SEVERITY	FILE NAME
	09/30 12:56:26	virus	Eicar Test File	WS-NET	VLE	10.1.0.10			89.238.73.97			443	web-browsing	alert	medium	eicar.com
	09/30 12:53:56	virus	Eicar Test File	WS-NET	VLE	10.1.0.10			89.238.73.97			443	web-browsing	alert	medium	eicar.com
	09/30 12:43:41	virus	Eicar Test File	WS-NET	VLE	10.1.0.10			89.238.73.97			443	web-browsing	alert	medium	eicar.com
	09/30 12:40:01	virus	Eicar Test File	WS-NET	VLE	10.1.0.10			89.238.73.97			443	web-browsing	alert	medium	eicar.com
	09/30 12:39:26	virus	Eicar Test File	WS-NET	VLE	10.1.0.10			89.238.73.97			443	web-browsing	alert	medium	eicar.com
	09/30 12:38:21	virus	Eicar Test File	WS-NET	VLE	10.1.0.10			89.238.73.97			443	web-browsing	alert	medium	eicar.com
	09/30 12:33:11	virus	100000	WS-NET	VLE	10.1.0.10			89.238.73.97			443	web-browsing	alert	medium	eicar.com

Kuvio 18. Lokit eicar testitiedostosta.

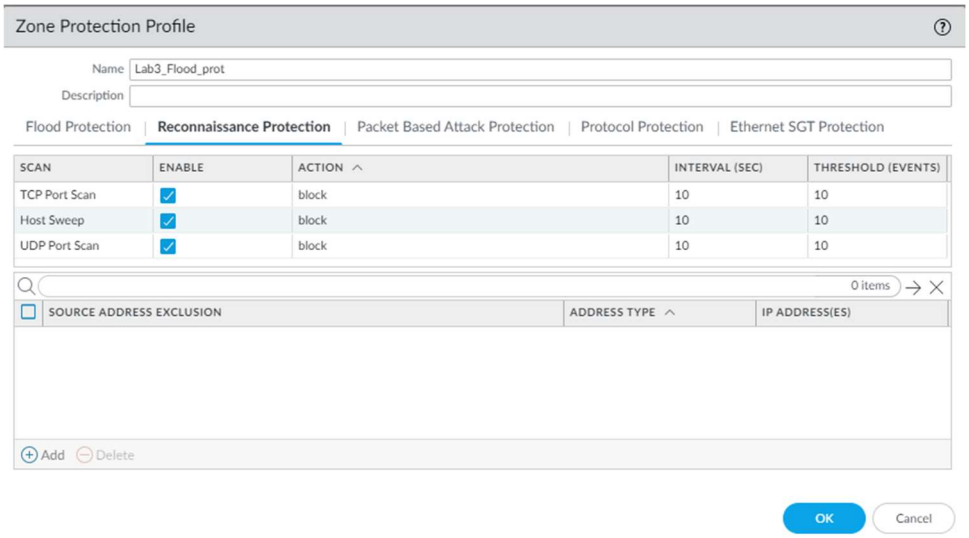
5 Flood Protection

Flood protection oli ekstratehtävänä tehtävänannossa, mutta päätimme tehdä tämänkin osan. Tässä tehtävänantona oli laittaa molemmat suojaukset, flood protection ja reconnaissance protection, päälle ja testata nmap skannauksella reconnaissance protectionia. Flood protection on DoS/DDoS:sia varten, ja se suojaa palvelunestohyökkäyksiltä tiputtamalla uusia yhteyksiä. Flood protectionin voi konfiguroida monella tavalla, mutta jätimme sen oletusasetuksille. Emme sitä enempää testannut, koska se ei ollut tehtävänannossa, emmekä uskoneet, että VLE ympäristön virtuaalikoneita saa DoS:ta, vaikka se olisi kokeilumielessä (ks. Kuvio 19) (Flood Protection N.d.).



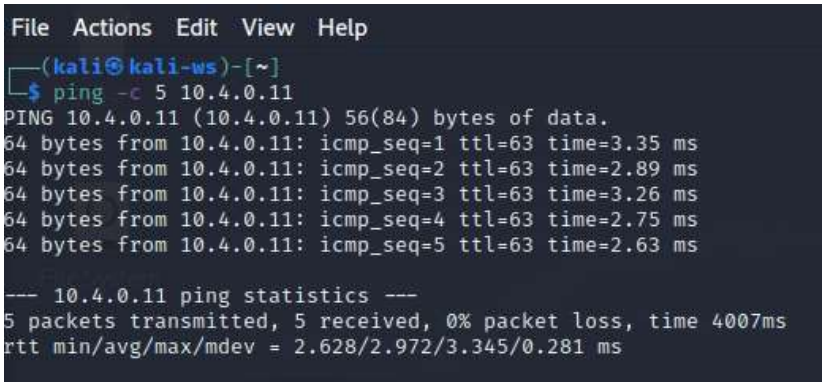
Kuvio 19. Flood Protection Settings.

Reconnaissance Protection suojaa “tiedustelulta”, eli esim. porttien skannaukselta. Määritimme asetukset jokaiseen mahdolliseen skannaukseen toiminnaksi “Block”, Intervalliksi 10 sekuntia, joka tiputtaa liikenteen tulevasta IP-osoitteesta 10 sekunniksi, ja thresholdiksi asetimme 10, eli 10 tapahtuman jälkeen toiminto tekee jotain, esim. 10 portin skannauksen jälkeen liikenne estetään 10 sekunniksi (ks. Kuvio 20) (Configure Reconnaissance Protection N.d.).



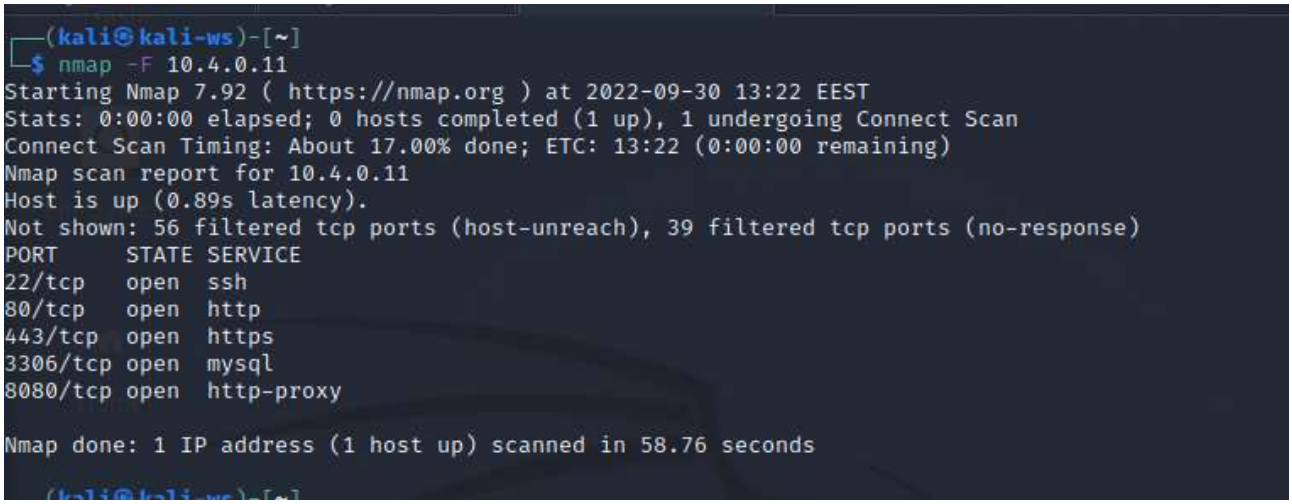
Kuvio 20. Zone Protection Reconnaissance Protection.

Reconnaissance protectionia testasimme tekemällä nmap skanneja Admin-Netistä olevalta kali virtuaaliselta koneelta DMZ-Zonella olevaan WWW virtuaaliseen koneeseen. Ennen kuin aloitimme kuitenkin skannaukset ja reconnaissance protectionin kokeilemisen, testasimme ensin miltä alkutilanne näyttää, ja että saisimme yhteyden Zonejen välillä. Yhteyden testaaminen onnistui pingaamalla kalista www-serverille (ks. kuvio 21).



Kuvio 21. Ping menee läpi kalista kohdekoneeseen.

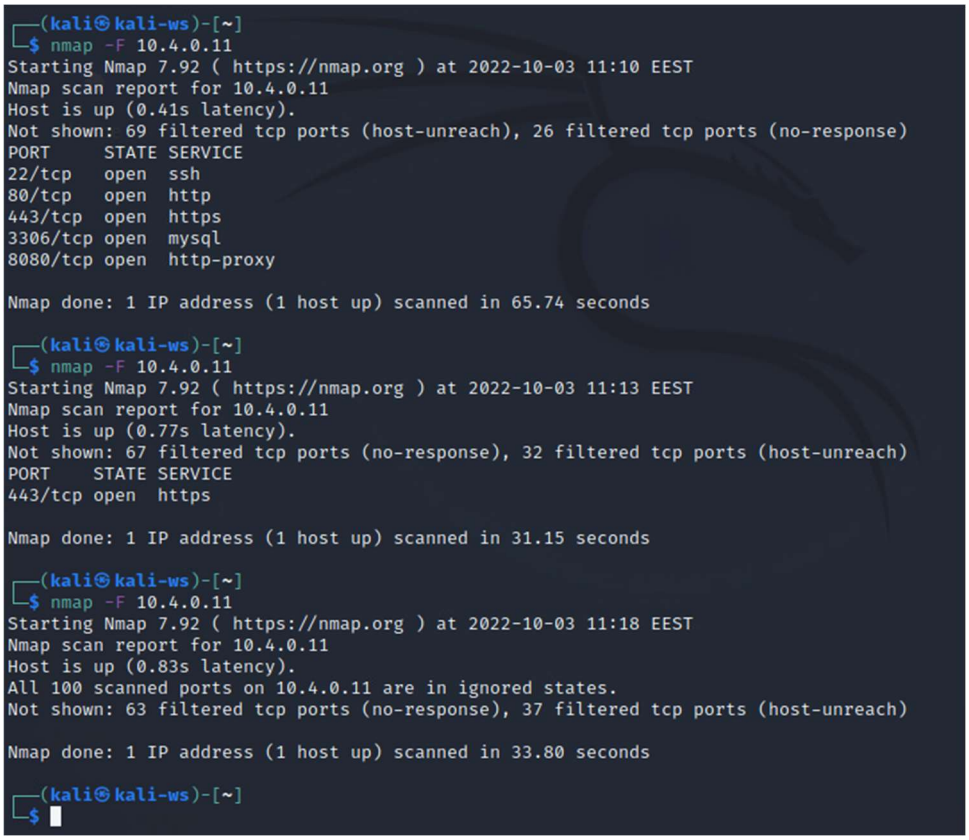
Pingin jälkeen kokeilimme myös tehdä nmapin eli porttiskannauksen ennen kuin committasimme Zone Protection profiilin, jotta pystymme vertaamaan alku- ja lopputilannetta nmap skannauksissa (ks. kuvio 22).



Kuvio 22. Nmap ennen sääntöjä.

Kun vihdoinkin committasimme Zone Protection profiilin, niin niiden pitäisi vaikuttaa nmapin skannaukseen. Valitettavasti näillä Reconnaissance Protection säännöillä saimme vaihtelevia tuloksia

nmapin toimivuudesta. Joissain yrityksissä palomuurin block toiminto toimii, mutta toisilla yrityksillä nmap löysi kaikki avoimet portit ja niiden palvelut. Joskus nmap löysi toisella yrityksellä yhden portin ja joillain yrityksillä ei yhtään porttia. Käytimme myös nmap komennoissa näkyvää “-F” komentoa, minkä avulla nmap käy vain 100 yleisintä porttia läpi, mikä nopeuttaa prosessia paljon. Normaalisti nmap käy läpi 1000 yleisintä porttia (ks. Kuvio 23).



Kuvio 23. Nmap skanneja.

Meidän saamat tulokset vaihtelivat todella paljon, ilman että teimme mitään muutoksia palomuuriin. Kun otimme nmapista satunnaisen järjestyksen pois, eli lisäsimme ”-r” nmap komentoon, aloimme saamaan yhteneviä tuloksia. Komennolla “nmap -r $IP” ei enää käy portteja läpi satunnaisessa järjestyksessä vaan aina samassa järjestyksessä. Huomasimme, että nmap löysi aina samat portit, kun järjestys ei ollut satunnainen (ks. kuvio 24) (Port Specification and Scan Order N.d.).

```
┌──(kali㉿kali-ws)-[~]
└─$ nmap -F -r 10.4.0.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-03 12:05 EEST
Nmap scan report for 10.4.0.11
Host is up (0.75s latency).
Not shown: 73 filtered tcp ports (host-unreach), 22 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 69.91 seconds

┌──(kali㉿kali-ws)-[~]
└─$ nmap -F -r 10.4.0.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-03 12:06 EEST
Nmap scan report for 10.4.0.11
Host is up (0.58s latency).
Not shown: 75 filtered tcp ports (host-unreach), 20 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 70.35 seconds

┌──(kali㉿kali-ws)-[~]
└─$ nmap -F -r 10.4.0.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-03 12:08 EEST
Nmap scan report for 10.4.0.11
Host is up (0.50s latency).
Not shown: 76 filtered tcp ports (host-unreach), 19 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 70.92 seconds
```

Kuvio 24. Nmap skannit ilman satunnaisuutta ja ”-r” komennolla.

Oletamme tämän johtuvan intervalli ja threshold asetuksista, koska satunnaisella järjestyksellä tuli satunnaisia tuloksia, ja niitä muottamalla pystyttiin vaikuttamaan vähän tuloksiin. Lokeista pystyimme myös näkemään, kuinka 10 sekunnin jälkeen palomuuri antaa uuden ilmoituksen ja blokkaa taas seuraavaksi 10 sekunniksi (ks. Kuvio 25).

Kuvio 25. logit nmap skannauksista.

Pelkällä blockilla ei voi estää nmappia. Nmapin saa konfiguroitua niin, että se skannaa portteja niin hitaasti ja mahdollisimman huomaamattomasti, ettei siitä jää selkeitä jälkiä, ja jos nmapin kohteena olevaa serveriä haluaa pitää toimivana, esimerkiksi webbisivupalveluna, näitä hitaita ja huomaamattomia pyyntöjä ei voi estää. IP blockauksella nmapin esto onnistuisi vähän paremmin, yhteys katkeaisi, mutta tämäkin skannaus pitäisi palomuurin ensin havaita, jonta nmap oikein konfiguroituna ei triggeröi. Sen lisäksi meidän mielestämme tämä Zone Protection on tehty enemmän DoS/DDoS hyökkäyksiä varten, eikä skannauksia varten (Cucos. 2021).

6 Pohdinta

Labra lähti hyvin käyntiin, ohjeet olivat selkeät ja pääsimme heti työntekoon. Työntekoa helpotti myös opettajan ennakkoon tekemät videomateriaalit, joista näki paremmin mitä piti tehdä. Tässä labrassa tuli taas paljon uutta kiinnostavaa tietoa palomuurin käytöstä. Labrojen tekeminen tuntuu helpottuvan, kun joka labrassa saa paremman käsityksen siitä, miten palomuuri toimii ja miten eri asetusten muuttaminen vaikuttaa mihinkin.

Opimme uusien turvallisuuspolitiikkojen profiilien käytöstä ja uusien sääntöjen luomisesta, ja tämän takia meillä on mielestämme parempi käsitys uhkien estämisestä ja eri termeistä palomuurissa esimerkiksi vulnerability protection ja file blocking. Yhdessä kohtaa oli hieman epäselvyyttä, kun video ja ohje olivat hieman ristiriidassa toistensa kanssa, mutta tämäkin saatiin selvitettyä opettajalta.

Ekstratehtävässä oli hieman pähkäilemistä, siitä miten skannaaminen toimii nmapin kanssa ja millä tavalla block toiminto toimii Palo Alton palomuurissa. Käytimme nmapin ja palomuurin reconnaissance protectionin asetusten kokeiluun paljon aikaa, ihan omasta mielenkiinnosta. Opimme paljon uutta mielenkiintoista nmapista.

Lähteet

Configure Reconnaissance Protection N.d. Viitattu 3.10.2022 https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-reconnaissance-protection

Cucos L. 2021 15 NMAP Timing Options – When And How To Use Them 15.05.2021 Viitattu 3.10.2022 https://nudesystems.com/nmap-timing-options-when-and-how-to-use-them/

Decrypt or Die! Blogikirjoitus decryptaamisesta. 01.08.2017. Viitattu 3.10.2022. https://www.elisasantamonica.fi/ajankohtaista/blogit/decrypt-or-die

Flood Protection N.d. Viitattu 3.10.2022 https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles/flood-protection

Lab 3 ohjeet. N.d. Viitattu 27.09.2022. https://moodle.jamk.fi/pluginfile.php/790760/course/section/81507/LAB2.pdf

Nmap: Discover your network N.d. Viitattu 30.9.2022 https://nmap.org/

Paloalto techdocs. About WildFire. 2.6.2022. Viitattu 3.10.2022. https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/about-wildfire

Paloalto techdocs, PAN-OS Web Interface Reference. N.d. Viitattu 3.10.2022. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles-vulnerability-protection

Paloalto techdocs. Security profiles. N.d. Viitattu 3.10.2022. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/security-profiles

Paloalto techdocs. Set Up File Blocking. 13.9.2022. Viitattu 3.10.2022. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/set-up-file-blocking

Paloalto techdocs. Threat Details. N.d. Viitattu 3.10.2022 https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/web-interface-basics/threat-details

Paloalto techdocs. What is URL Filtering? N.d. Viitattu 3.10.2022. https://www.paloaltonetworks.com/cyberpedia/what-is-url-filtering

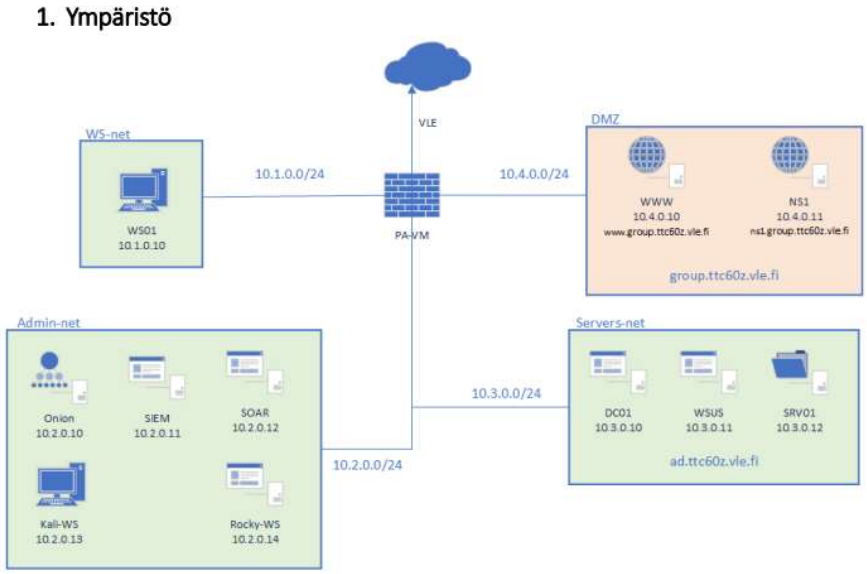
Port Specification and Scan Order N.d. Viitattu 3.10.2022 https://nmap.org/book/man-port-specification.html

Timing and Performance N.d. Viitattu 3.10.2022 https://nmap.org/book/man-performance.html

What is Kali Linux? 09.09.2022. Viitattu 30.9.2022 https://www.kali.org/docs/introduction/what-is-kali-linux/#kali-linux-features

Liitteet

Liite 1. Labraympäristö



Kuvio 1 Laboratorio ympäristö