Omaisuuden hallinta

Harjoitustyö 1

Antti Tammelin, AA4493

Tero Räsänen, AA4054

Elmeri Söderholm, AA3979

Eliel Taskinen, AA3737

Harjoitustyö

Kyberturvallisuuden hallinta TTC6020-3002, Jarmo Nevala

7.12.2022

Tieto- Ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

1 Johdanto 2
2 Yritys 2
2.1 Tausta 2
2.2 Käytännöt 2
3 Ympäristö 3
4 Ympäristön erilliset osat 4
4.1 WS-Net 4
4.2 DMZ 4
4.3 Admin-net 4
4.4 Servers-net 5
4.5 PA-VM 5
5 Työkalut 5
6 Pohdinta 6
Lähteet 7
Liitteet 8
Liite 1. Ympäristön kuvaus 8

Kuviot

Kuvio 1. Väärä kappale. 6

Taulukot

Taulukko 1. Ympäristön virtuaaliset koneet. 3
Taulukko 2. Ympäristön työkalut. 6

1 Johdanto

Tämä harjoitustyö on osa Kyberturvallisuuden hallinta -opintojaksoa ja tässä dokumentissa teemme omaisuuden hallinnan Kyberturvallisuus-moduulissa käytetystä VLE-ympäristöstä. Tämä omaisuuden hallinta on luotu pohjautuen ISO 27001 (taulukko A.8.1) ja 27002 (kappale 8.1) standardeihin ja dokumentissa käymme läpi ympäristöön liittyvät omaisuudet, johon lukeutuu tiedolliset ja fyysiset omaisuudet, sekä myös ohjelmistot, työkalut ja palvelut. Näiden lisäksi omaisuuksiin kuuluu myös ihmiset kuten ympäristön käyttäjät. Käytimme tässä raportissa vuonna 2022 julkaistuja standardeja, koska tieto väärästä tiedosta ohjeissa tuli vasta harjoituksen tekemisen jälkeen. Mielestämme asiat kuitenkin pätevät vuonna 2017 julkaistuun standardiin. Raportissa voi kuitenkin olla puutteita.

2 Yritys

2.1 Tausta

DefendByVirtual, joka harjoituksen ajaksi on ympäristön omistaja, aloitti toimintansa 2021. Yrityksellä on monenlaisia puolustusmekanismeja, SIEM, SOAR, palomuuri. Meidät palkattiin vuonna 2022 auditoimaan ja saamaan pystyyn heitteille jätetty yritys. Yrityksellä ei ole yhtään rahaa, ja ei voi investoida enempiä resursseja kuin meidän ryhmältämme löytyy.

2.2 Käytännöt

Koko ympäristön omistaa DefendByVirtual ja se sisältää monta eri verkkoa, joissa on eri käyttötarkoituksiin kuuluvia laitteita. Yrityksellä on vastuu perehdyttää työntekijät turvallisuusvaatimuksiin ja menettelyihin, joilla suojataan päätelaitteita kuten esimerkiksi kirjautumismenetelmät sekä palveluiden sammuttaminen. Työntekijöitä perehdytetään myös arkaluonteisen tiedon käsittelyyn sekä eri tekniikoihin, jolla suojataan omaa päätelaitetta.

Ympäristöön kuuluu Palo Alto -palomuuri, jolla suojataan yrityksen tietojärjestelmiä erilaisilla konfiguraatioilla. Kaikkiin verkkojen tietojärjestelmiin tehdään kovennuksia, jotta tietomurtojen mahdollisuus pienenee. Yrityksellä on eri henkilöillä erilaisia vastuita. Yrityksen ylläpidolla on vastuu pitää kaikki laitteet toiminnassa sekä hallita päivityksiä. Mahdollisista häiriöistä ilmoitetaan muulle

henkilökunnalle. Laitteissa on varmuuskopiointi käytössä, jotta mahdolliset menetetyt tiedot voidaan palauttaa. Ympäristön päätelaitteet pitää rekisteröidä ja pitää listaa niiden versioista sekä mahdollisista muutoksista.

Käyttäjien verkkotoimintaa pitää suojata ja rajata, jotta mahdollisilta haittaohjelmilta vältytään. Muilla työntekijöillä on myös vastuu pitää kirjautumistiedot salassa sekä pitää virustorjunta ajan tasalla. Kirjautumistunnuksien vaatimukset täytyy olla baselinejen mukaisia sekä salasanan vaihto täytyy olla mahdollista ylläpidon kautta. Fyysisten porttien (esim. USB-porttien) käyttöönotto sekä poisotto täytyy olla sallittua muistilaitteiden kanssa.

Suojattavaa omaisuutta pitää käyttää sääntöjen mukaan ja omistajuus pitää määrittää ja suojata jokaiselle laitteelle.

3 Ympäristö

Harjoitustyössä käytimme VLE ympäristöä, josta olimme lisänneet kuvat Liitteenä 1. Sen lisäksi keräsimme taulukon, missä lukee kaikki tarvittava tieto eri virtuaalisista koneista.

Zone	Name	Version	IP	Memory (MB)	Processor (CPUs)
Firewall	Palo Alto	PAN-OS 10.1	198.19.50.96	6144	2
WS-Net	WS01	Windows 11 Education	10.1.0.10	4096	2
Admin-Net	Onion	SentOS Linux 7 (Core)	10.2.0.10	16384	4
Admin-Net	SIEM	Rocky Linux 8.6 (Green Obsidian)	10.2.0.11	16384	4
Admin-Net	SOAR	Rocky Linux 8.5 (Green Obsidian)	10.2.0.12	16384	4
Admin-Net	Kali-WS	Kali 2021.4 & GVM 21.4.3	10.2.0.13	4096	2
Admin-Net	Rocky-WS	Rocky Linux 8.6 (Green Obsidian)	10.2.0.13	16384	4
Admin-Net	MISP	Rocky Linux 8.5 (Green Obsidian)	10.2.0.15	16384	4
Servers-Net	DC01	Windows Server 2019	10.3.0.10	4096	2
Servers-Net	WSUS	Windows Server 2019	10.3.0.11	4096	2
Servers-Net	SRV01	Windows Server 2019	10.3.0.12	4096	2
DMZ	NS1	Rocky Linux 8.6 (Green Obsidian)	10.4.0.10	1024	1
DMZ	WWW	Rocky Linux 8.5 (Green Obsidian)	10.4.0.11	1024	1

Taulukko 1. Ympäristön virtuaaliset koneet.

4 Ympäristön erilliset osat

4.1 WS-Net

WS-net verkko sisältää WS01-nimisen laitteen, joka toimii organisaation workstation koneena. Laitteessa on käytössä Windos 11 Education käyttöjärjestelmä ja laitetta käyttää pääsääntöisesti organisaation työntekijä, jolla ei välttämättä ole käyttöoikeuksia muihin laitteisiin tai verkkoihin. WS-Netin subnetti on 10.1.0.0/24.

4.2 DMZ

DMZ, eli demilitarisoitu alue on organisaation ympäristössä oleva tietoturvaan liittyvä fyysinen tai looginen aliverkko. Se on erillinen aliverkko, joka sisältää organisaation ulospäin suuntautuvat palvelut. DMZ sisältää WWW ja NS1 virtuaaliset koneet, joista WWW koneella on webbisivupalvelu, ja NS1 toimii DNS:nä. DMZ subnetti on 10.4.0.0/24.

4.3 Admin-net

Admin-net on organisaation ylläpitäjän käytössä oleva verkko, johon kuuluu erilaisia laitteita ja palveluita. Näillä voi muun muassa vahvistaa ympäristön tietoturvaa, hallita muita laitteita ja seurata lokeja. Admin-Net subnetti on 10.2.0.0/24.

Admin-Netissä on eniten virtuaalisia koneita ja palveluita. Tässä Zonessa sijaitsee monenlaisia tietoturvaan tarpeellisia palveluita, jotka mahdollistavat verkon valvomisen, ja mahdollisen tietoturvallisen testaamisen. Admin-Netissä on SIEM ja SOAR, jotka ovat vastuussa SOC:in pyörittämisestä ympäristössä. SIEM, eli Security Information and Event Management, on palvelu, joka kerää ja analysoi eri hälytyksiä eri lähteistä. SOAR auttaa SIEM:iä hälytysten automatisoinnissa.

Näiden lisäksi Admin-Netissä sijaitsee Kali-WS, mitä käytetään linux koventamisen esimerkkiä, ja millä pystyy kokeilemaan erilaisia penetration testing keissejä ympäri VLE ympäristöä. Admin-Netissä on myös Virtuaaliset koneet Onion, Rocky-WS ja MISP, joita emme ole vielä käyttäneet, joten emme tiedä mitä niiden pitäisi tehdä.

4.4 Servers-net

Servers-net on verkko ympäristössä, joka sisältää organisaation palvelimet, joita käytetään ympärisön hallitsemisessa. Servers-Netissä sijaitsee DC01, WSUS ja DC01. DC01 on Domain Controller Active Directorylle, SRV01 on tiedostoserveri, johon menee meidän varmuuskopioinnit, ja WSUS joka on myös Domain Controller ja hallitsee päivityksiä WS01:lle. Servers-net subnetti on 10.3.0.0/24.

4.5 PA-VM

PA-VM on ympäristön Palo Alto palomuuri, jolla hallitaan koko organisaation verkkoliikennettä. Palomuurin ip on 198.19.50.96.

5 Työkalut

DefendByVirtualin ympäristössä on monenlaisia eri työkaluja, joita käytetään monissa eri tilanteissa. Dokumentoimme kaikki, mitä asiakas pyysi ja mitä muita löysimme. Dokumentoimme kaikista työkaluista niiden nimen, version, käyttötarkoituksen, tehtävän, ja mihin ne ovat yhteydessä.

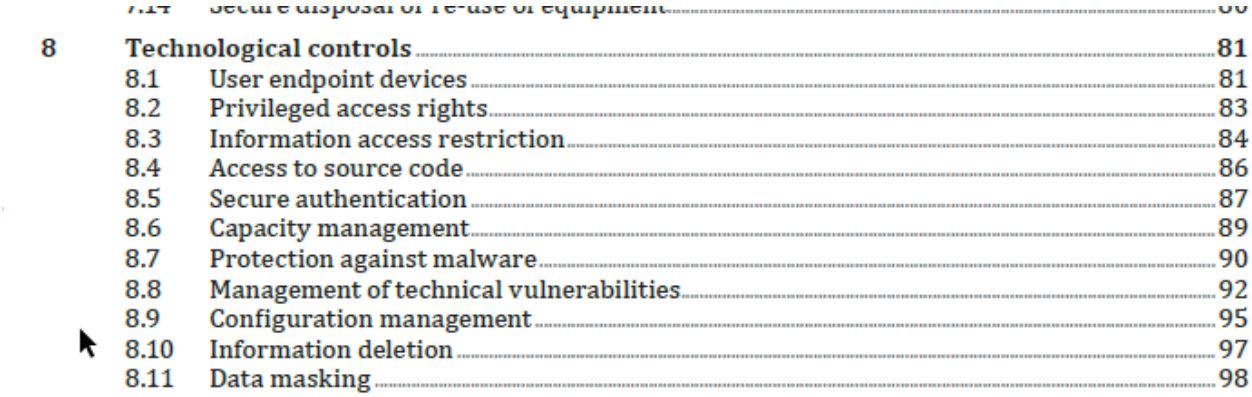
Työkalu	Versio	Käyttötarkoitus	Tehtävä	Yhteydet
Palo Alto	PAN-OS 10.1	Palomuuri	Hallita verkkoliikennettä	VLE, WS-net, DMZ, Admin-net, Servers-net
Wazuh	4.3.6	SOAR	Automatisoida hälytyksiin reagointi	VLE, DMZ, WS-net
iTop	3.0.1	VPN, tietojen palautus, yksityinen selain		VLE, DMZ, WS-net
MISP	2.4.161	Open source uhkien tiedustelu	Uusien uhkien tiedustelu	VLE, DMZ, WS-net
Security Onion	2.3.140	IDS, turvallisuuden ja logien hallinta	Koko verkon turvallisuuden valvonta	VLE, DMZ, WS-net
Green-Bone		Haavoittuvuuden hallinta	Haavoittuvuuksien skannaus	VLE, DMZ, WS-net
TheHive		Incident response alusta		VLE, DMZ, WS-net
Elastic	8.3.3	SIEM	Logien visualisointi ja hälytykset	VLE, DMZ, WS-net
Shuffle	1.0	Visuaalinen editointityökalu		VLE, DMZ, WS-net
Cortex	3.1.6-1	Analysointi	Analyysityökalu	VLE, DMZ, WS-net

Jupyterlab	3.3.2	Verkkopohjainen kehitysympäristö		VLE, DMZ, WS-net
Docker	20.10.21	Kontitus	Pitää verkkosivut yllä	VLE
Wordpress	6.1	WWW-sivu	Verkkosivu	VLE

Taulukko 2. Ympäristön työkalut.

6 Pohdinta

ISO standardeista ei ollut hirveästi apua. Sen lisäksi meidän ISO Standardeissa ISO 27002 kappaleessa 8.1. ei ollut mitään hyödyllistä. Sen kappaleen nimi piti olla Asset Management, Responsibility for assets, mutta se oli Technological Controls, User Endpoint Devices (ks. kuvio 1). Tämä johtuikin siitä, koska standardit olivat vanhentuneet ohjeissa.



Kuvio 1. Väärä kappale.

Sen lisäksi tämä harjoitustyö oli hankala aloittaa, koska tehtävänanto oli hyvin suppea. Seuraavalle tekokerralle miettisin kokonaan labran uusiksi, tai esimerkiksi antaisin esimerkkimallin hyvästä omaisuuden hallinta raportista, että opiskelijoilla olisi jotain minkä pohjalta lähteä tekemään.

Omaisuuden hallinta on organisaatiolle tärkeä osa-alue, joten tämän aiheen opiskelukin on tärkeää. Koska standardeja on niin suuri määrä, ei niitä pysty opettelemaan kaikkia kerralla. Siksi tämän harjoituksen tyyppinen keskittyminen tiettyihin standardeihin on hyvä idea. Kuten edellisessä kappaleessa kerroimme, parempi ohjeistus harjoitustyöhön tai esimerkkien antaminen olisi ollut hyödyllistä. Nyt tuntui, että ryhmämme aloitti harjoituksen tekemisen kokonaan tyhjästä ja se vaikutti aika paljon harjoituksen tekemiseen ja lopputulokseen.

Lähteet

Digiturvamalli. N.d. Viitattu 28.11.2022. https://www.digiturvamalli.fi/vaatimus/8-asset-management

Cortex 7.10.2022 https://github.com/TheHive-Project/Cortex/milestone/32

Liitteet

Liite 1. Ympäristön kuvaus