Haavoittuvuuksien hallinta

Harjoitustehtävä 2

Aro Jesper, TTV21S1

Jalkanen Kalle, TTV21S2

Koivisto Ossi, TTV21S2

Salomäki Sini, TTV21S5

Harjoitustehtävä

Kyberturvallisuudenhallinta TTC6020-3006, Nevala Jarmo

xx.2.2024

Tieto- ja viestintätekniikka, insinööri (AMK)

Sisältö

[1 Johdanto 3](#_Toc160541627)

[2 Teknisten haavoittuvuuksien hallinta 3](#_Toc160541628)

[2.1 Tunnistaminen 3](#_Toc160541629)

[2.2 Arviointi 4](#_Toc160541630)

[2.3 Käsittely 4](#_Toc160541631)

[3 Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin 5](#_Toc160541632)

[3.1 Tarkoitus 5](#_Toc160541633)

[3.2 Asentaminen 6](#_Toc160541634)

[4 Haavoittuvuuksien skannaus 6](#_Toc160541635)

[4.1 WS ja ADMIN-net 6](#_Toc160541636)

[4.2 DMZ 10](#_Toc160541637)

[4.3 Servers-net 11](#_Toc160541638)

[5 Riskianalyysi 12](#_Toc160541639)

[5.1 Haavoittuvaisuudet 12](#_Toc160541640)

[5.2 Suositellut korjaukset 12](#_Toc160541641)

[6 Pohdinta 13](#_Toc160541642)

[Lähteet 14](#_Toc160541643)

Kuviot

[Kuvio 1 ohjelmistot 4](#_Toc160541644)

[kuvio 2. Greenbone skannerin vertailu tietokantojen versiot 7](#_Toc160541645)

[kuvio 3 greenbonen antamat avonaiset portit 7](#_Toc160541646)

[kuvio 4 Greenbone ws tulokset 7](#_Toc160541647)

[kuvio 5 nmap WS-net tulokset 8](#_Toc160541648)

[kuvio 6 ws1 haavoittuvaisuudet 8](#_Toc160541649)

[kuvio 7. Onion haavoittuvaisuudet 8](#_Toc160541650)

[kuvio 8. SIEM haavoittuvaisuudet 9](#_Toc160541651)

[kuvio 9 SOAR haavoittuvuudet 9](#_Toc160541652)

[kuvio 10 rocky haavoittuvaisuudet 9](#_Toc160541653)

[kuvio 11 Kalin haavoittuvaisuudet 10](#_Toc160541654)

[kuvio 12. WWW havoittuvaisuudet 10](#_Toc160541655)

[kuvio 13. NS1 haavoittuvaisuudet 11](#_Toc160541656)

[kuvio 14. SRV01 haavoittuvaisuudet 11](#_Toc160541657)

[kuvio 15. DC01 haavoittuvaisuudet 11](#_Toc160541658)

[kuvio 16. Nmap skannaus wsus laitteesta 12](#_Toc160541659)

Taulukot

Kuvaotsikkoluettelon hakusanoja ei löytynyt.

[Taulukko 1 Laitteiden kriittisyys 5](#_Toc159329129)

# Johdanto

Tässä harjoituksessa tavoitteena on muodostaa ISO standardin 27001 ja 27002 mukainen haavoittuvuuksien hallinta kuvitteelliselle organisaatiollemme. Hallinta suunnitelma pitää sisällään ISO standardin kohdan 8.8. mukaiset vaatimukset teknisten haavoittuvuuksien hallinnasta, kohdan 8.19 mukainen ohjeistus ohjelmistojen asentamisesta organisaation järjestelmiin, haavoittuvuuksien skannauksen Greenbone Vulnerabilityllä ja tulosten dokumentoinnin sekä riskianalyysin, jossa käy ilmi mitkä ympäristön haavoittuvuudet huomioidaan. Dokumentin tarkoituksena on selkeyttää organisaatiomme menettelytapoja haavoittuvuuksien tunnistamisessa, hallinnassa ja niiden ehkäisevissä toimenpiteissä.

# Teknisten haavoittuvuuksien hallinta

Hallintakeinon tyyppi on ehkäisevä eli näillä toimilla pyritään ehkäisemään mahdollisimman paljon potentiaalisi uhkia. Tarkoituksena on etukäteen kerätä tietoa organisaation käytössä olevien tietojärjestelmien haavoittuvuuksista, jotta niitä voidaan tarkastella kunkin haavoittuvuuden tasolle sopivalla vakavuudella. Näin ollen voidaan estää teknisten haavoittuvuuksien hyväksikäyttö. (SFS-EN ISO/IEC 270032:2022, 102)

## Tunnistaminen

Jotta tunnistamista voidaan tehdä, Organisaatiolla on ylläpidossaan ISO standardin kohtien 5.9–5.14 mukainen omaisuuserien luettelo. Omaisuuserien luettelossa luetellaan organisaation käytössä olevat ohjelmat, joiden lisäksi ohjelman toimittaja, nimi, versio, käyttötilanne ja vastaava henkilö organisaatiossa (kuvio 1). Omaisuuserien listaa tulee vastuuhenkilön päivittää sen mukaan, kun muutoksia tapahtuu (SFS-EN ISO/IEC 270032:2022, 102).

Kuva, joka sisältää kohteen teksti, Fontti, viiva, numero

Kuvaus luotu automaattisesti

Kuvio 1 ohjelmistot

Kunkin ohjelmiston vastuuhenkilö tarkastaa viikoittain oman vastuualueensa ohjelmistojen turvallisuuden. Yrityksen tietoturvatiimi seuraa myös aktiivisesti ajantasaisia tietoturvauutisia esimerkiksi kyberturvallisuuskeskuksen -sivuja (https://www.kyberturvallisuuskeskus.fi/fi) ja tutkii niissä ilmenneiden haavoittuvuuksien soveltuvuutta organisaatiomme ympäristöön. Toimittajan valinnassa tulee kiinnittää huomiota, että heillä on käytössä asianmukaiset raportointi ja tunnistus menetelmät haavoittuvuuksille. Lisäksi organisaatiossamme tulee olla ajantasaiset työkalut haavoittuvuuksien tunnistamiselle, organisaation käytössä on Greenbone Security scanner (versio 22.4.0), jokaisen haavoittuvuuden korjauksen jälkeen organisaation vastuuhenkilön on pystyttävä todentamaan, että korjaus on tehonnut.

## Arviointi

Teknisiä haavoittuvuuksia koskevissa raporteissa kyseisestä ohjelmistosta tai ohjelmistoista vastaava henkilö tai henkilöt sekä tietoturvapäällikkö suorittavat raportin analysoinnin ja mikäli mahdollinen haavoittuvuus löytyy, on siihen liittyvät riskit yksilöitävä ja tehtävä tarvittavat toimenpiteet liiketoiminnan suojelemiseksi.

## Käsittely

Organisaatiossa tunnustettuihin ja ilmotettuihin haavoittuvuuksiin tulee reagoida vuorokauden sisässä. Mikäli haavoittuvuus on suuri tai merkittävä riski liiketoiminnalle ragoida täytyy välittömästi. Organisaatiossa on sovittu, että käytetään oletuksena kaikissa ohjelmistoissa automaattisia päivityksiä, mikäli ohjelmisto sen sallii. Haavoittuvuuden paikkaamiseen tulee käyttää vain luotettuja lähteitä ja korjausmenetelmiä, luotetut lähteet voivat olla niin organisaation sisäisiä kuin ulkoisiakin esimerkiksi toimittajan tarjoamat ratkaisut, jotka yleensä ovat päivitys tai korjaustiedostoja. Mikäli haavoittuvuus koskee laajalti koko organisaation laitteita tai osaa niistä, on korjaus toimenpiteet aloitettava yritystoiminnalle kriittisimmästä laitteesta (taulukko 1).

Taulukko 1 Laitteiden kriittisyys

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Priority 1** | **Priority 2** | **Priority 3** |
| **Palvelimet** | DC01  SRV01  WSUS  PaloAlto | ns-1  www | Onion  SIEM  SOAR  OVS |
| **työasemat** |  | Kali-WS (admin-net)  Rocky-WS (admin-net) | WS01 (WS-net) |

Mikäli tarjolla ei ole korjaus vaihtoehtoa tai sitä ei olla vielä julkaistu, organisattio ottaa käyttöön muun hallinta keinon, jotka on määritelty listassa järjestyksessä.

Hallintakeinot mikäli korjaus vaihtoehtoa ei ole saatavilla luotetusta lähteestä

1. Ohjelmiston toimittajan suosittelema kiertoratkaisu
2. Haavoittuneen palvelun pois käytöstä otto.
3. Haavoittuvuuden estäminen palomuurin kautta
4. Haavoittuneen kohteen suojaaminen haitalliselta liikenteeltä
5. Valvonnan ja viestinnän lisääminen, jotta voidaan havaita hyökkäys

# Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin

## Tarkoitus

Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin on ehkäisevä hallintakeinon tyyppi, jolla hallitaan turvallisesti ohjelmistojen asentamista järjestelmiin. Asentamalla varmistetaan järjestelmien eheys ja estetään mahdollisten teknisten haavoittuvuuksien hyödyntämisen sekä ylläpidetään toimittajien tuki ohjelmistolle.

## Asentaminen

Ohjelmien ja päivitettyjen versioiden asentamisessa kuuluu olla tiedossa ohjelmistoa edeltävät ohjelmat sekä versiot dokumentoinnin sekä mahdollisten palautusstrategioiden kannalta. Asennetut ohjelmat pitää sisältää vain hyväksyttyä suorituskelpoista koodia ja koulutetun pääkäyttäjän toimesta. Uusien versioiden käyttöönotossa pitää selvittää version turvallisuus sekä sen tietoturvahaavoittuvuuksien määrä.

Ennen ohjelmiston asennusta pitää ohjelmisto ja päivitykset testauttaa ympäristössä, mahdollisten haavoittuvuuksien, yhteensopimattomuuksien tai muiden ongelmien varalta. Lisäksi kaikki ohjelmistojen vanhat versiot arkistoidaan varatoimenpiteenä, tarvittavien tiedostojen sekä konfiguraatioiden kanssa, niin pitkään kun se on mahdollista. Tässä vaiheessa kuuluu myös päivittää kaikki vastaavat ohjelmistojen lähdekirjastot ja määritetään palautusstrategia, mikäli sitä tarvitaan.

Ohjelmistojen versioita on päivitettävä siten, että toimittajien tuki säilyy, sillä ohjelmisto, jonka tuki on päättynyt, on tietoturvallisesti heikompi sekä mahdollinen apu on tällöin olematon. Organisaation on myös otettava huomioon avoimen lähdekoodin ohjelmistojen käytön riskit ja tuen mahdollinen loppuminen tai puute. (SFS-EN ISO/IEC 27002:2022, 120, 121)

# Haavoittuvuuksien skannaus

Aloitimme skannaamanaan Admin-net ympäristöä greenbone security scannerilla (versio 22.4.0) ja skannaus parametrit ja vertailu tietokantojen versiot (kuvio 2).

## WS ja ADMIN-net

Ajoimme skannit laite kerrallaan ympäristössämme ja ensimmäinen laite olikin WS01. Tuloksista näkyy, että laitteella oli 2 porttia auki greenbonenen mukaan (kuvio 3) ja 4 porttia nmap:in mukaan (kuvio 4). Laitteella oli myös haavoittuvaisuuksia (kuvio 5). Seuraavaksi skannasimme Onion:in osoitteessa 10.2.0.10 ja löysimme haavoittuvaisuudet (Kuvio 6). Jatkoimme skannaamaan SIEM laiteen osoitteessa 10.2.0.11 (kuvio 8.). Seuraavaksi skannasimme SOAR:in osoitteesta 10.2.0.12, ja listasimme sen haavoittuvaisuudet (kuvio 9). Jatkoimme rocky-Ws:ään 10.2.0.14 ka otimme haavoittuvaisuudet ylös (kuvio 10). Viimeinen laite Admin verkossa oli Kali-WS 10.2.0.13 ja sen haavoittuvaisuudet ovat (kuviossa 11.)

Greenbonen tuloksia tarkastelemalla selviää, että Admin-net:issä suurimmat haavoittuvaisuutemme ovat JQuery haavoittuvaisuuksia ja heikkoja avain algoritmeja. Aiomme jatkossa puuttua näihin organisaatio tasolla ja poistaa heikot algoritmit käytöstä. Aiomme myös varmistaa, että pidämme JQueryä ajan tasalla.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

kuvio 2. Greenbone skannerin vertailu tietokantojen versiot

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, viiva

Kuvaus luotu automaattisesti

kuvio 3 greenbonen antamat avonaiset portit

kuvio 4 Greenbone ws tulokset

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

kuvio 5 nmap WS-net tulokset

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

kuvio 6 ws1 haavoittuvaisuudet

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

kuvio 7. Onion haavoittuvaisuudet

Kuva, joka sisältää kohteen teksti, Fontti, numero, kuvakaappaus

Kuvaus luotu automaattisesti

kuvio 8. SIEM haavoittuvaisuudet

Kuva, joka sisältää kohteen teksti, Fontti, numero, ohjelmisto

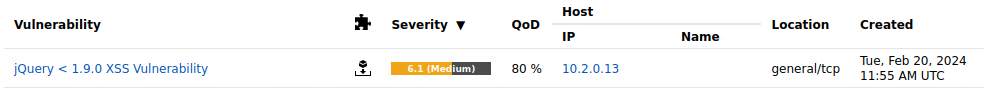
Kuvaus luotu automaattisesti

kuvio 9 SOAR haavoittuvuudet

Kuva, joka sisältää kohteen teksti, kuvakaappaus, numero, Fontti

Kuvaus luotu automaattisesti

kuvio 10 rocky haavoittuvaisuudet



kuvio 11 Kalin haavoittuvaisuudet

## DMZ

Aloimme skannaamaan DMZ-verkosta haavoittuvaisuuksia ja ensimmäisenä laitteena olikin organisaation WWW palvelin (kuvio 12). Pääasialliset haavoittuvaisuudet olivat heikot KEX algoritmit ja Itse www sivusta johtuneet varoitukset. Olemme aloittaneet jo kovennus toimenpiteet (kovennus kurssi 4. labra) ja tulevaisuudessa saammekin web sivujen turvallisuuden paremmaksi. Tällä hetkellä web palvelinta ajetaan Docker kontista, joten realistista riskiä koko järjestelmän kattavaan tietomurtoon ei synny.

NS1 laite ilmoitti myös heikoista avain algoritmeista (kuvio 13) , tulemme korjaamaan nämä haavoittuvaisuudet myöhemmin.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

kuvio 12. WWW havoittuvaisuudet

Kuva, joka sisältää kohteen teksti, Fontti, numero, viiva

Kuvaus luotu automaattisesti

kuvio 13. NS1 haavoittuvaisuudet

## Servers-net

Viimeiseksi aloimme tutkimaan server-net verkkoa ja ensimmäisenä laitteena srv01:stä (kuvio 14). Heti alkuunsa löysimme kriittisen haavoittuvaisuuden, jonka aiomme korjata heti. Domain controllerista ei taas löytynyt niin paljoa haavoittuvaisuuksia (kuvio 15), pääasiassa vanhentuneita protkollia.

Valitettavasti jouduimme käymään WSUS laitteen läpi vain nmap portti skannauksella (kuvio 16), sillä ilmeisesti käyttämässämme greenbone skannerissa on yhteensopivuus ongelmia kyseisen laitteen kanssa. Näistä ei löytynyt mitään yllättävää

Kuva, joka sisältää kohteen teksti, Fontti, numero, viiva

Kuvaus luotu automaattisesti

kuvio 14. SRV01 haavoittuvaisuudet

Kuva, joka sisältää kohteen teksti, Fontti, viiva, numero

Kuvaus luotu automaattisesti

kuvio 15. DC01 haavoittuvaisuudet

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

kuvio 16. Nmap skannaus wsus laitteesta

# Riskianalyysi

## Haavoittuvaisuudet

Skannaus tulosten perusteella suurin riski on servers-netin SRV01 laite. Tällä laitteella oli ympäristön ainut korkean riskin skannaus tulos ” Windows IExpress Untrusted Search Path Vulnerability” joka mahdollistaa koodin ajamisen järjestelmässä. Todennäköisimmin kuitenkin hyökkäyksen kohteena on www-palvelin, jossa on haavoittuvuus joka mahdollista DOS-hyökkäyksen. Palvelin myös käsittelee käyttäjiä, sekä salasanoja suojaamattomalla http-yhteydellä. Https yhteyden käyttöönotto ratkoisi nämä ongelmat, ja sallisi esim. viestien ja tunnuksien salauksen (Digimarkkinointi nd).

Admin-net ympäristössä todennäköisin kohde voisi olla Onion. Se sisältää Cross-site scripting (XSS) haavoittuvuuden, jonka hyödyntäminen on kohtalaisen helppoa. Haavoittuvuus johtuu jQuery:n vanhentuneesta versiosta.

## Suositellut korjaukset

Pidimme greenbone skannerista työkaluna, sillä mielestämme sen riskien pisteytys oli paikkansapitävää. Aiommekin alkaa korjaamaan ympäristöä pisteytyksien mukaan muodostuvassa prioriteetti järjestyksessä. Kriittisimpänä on saada SRV01 laite turvallisesti toimintaan. Tällä hetkellä olemme myös päivittämässä WWW palvelinta käyttämään https yhteyttä. Oletamme että näillä saamme kriittisimmät osuudet ajan tasalle.

Tämän jälkeen aiomme päivittää jokaisen ympäristön laitteen ajan tasalle ja tehdä uudet skannaukset. Oletamme että näillä saamme ympäristön hyvin toimintakuntoon.

# Pohdinta

Mielestämme tehtävä sujui mukavasti ja tekeminen tuki hyvin kurssin oppimistavoitteita. Selkeän työnjaon ja tehtävänannon avulla emme kohdanneet juurikaan ongelmia. Materiaali tuki työskentelyä hyvin ja koemme oppineemme paljon tästä tehtävästä. Greenbone skannausten tekeminen oli osittain työlästä, sillä ympäristöä oltiin aiemmin kovennettu ja joudimme purkamaan kovennuksia, jotta skannaukset saatiin onnistumaan.

Lähteet

Digimarkkinointi. Kannattaako https ottaa käyttöön?. Viitattu 5.3.2024. https://www.digimarkkinointi.fi/blogi/kannattaako-https-ottaa-kayttoon

ISO/IEC 27002. 2022.Information security, cybersecurity and privacy protection — Information security controls. Oline SFS. Viitattu 20.2.2024.