VERKON VALVONTA: YMPÄRISTÖ JA SUUNNITELMA

Johanna Hakonen

Sisällysluettelo

1 Johdanto

Kyberturvariskejä hallitaan esimerkiksi valvomalla tietoverkkoa hyödyntämällä erilaisia analysointityökaluja kuten Microsoftin/Windowsin monitorointi- ja raportointityökaluja kuten Windows Event Viewer sekä kolmannen osapuolen ohjelmia kuten Wireshark (Wireshark Foundation, Wireshark, 2025).

Tässä esitellään kevyt verkonvalvontasuunnitelma, joka tehtiin ChatGPT:n avulla (OpenAI, 2025). Osa suunnitelmasta toteutettiin ja ympäristönä käytettiin Windows-palvelinta ja -työasemaa sekä Kali ja Parrot Linux-koneita VMwaressa.

2 Ympäristön asennus

Lisättiin toimialueeseen viimeksi vuonna 2023 päivitetty työasema. Avattiin ensin uusi Windows 10 -työasema (wks1win10_22H2_x64-virtuaalikone) wks2-physio ja estettiin päivitykset Windows Updatessa. Päivitettiin VMware Toolsit ja sammutettiin kone. Avattiin palvelin ja työasema uudestaan.

Ethernet-asetuksista nähtiin, että kone löysi automaattisesti amidom-toimialueen ja DHCP jakoi automaattisesti osoitteen (192.168.100.128).

Kirjauduttiin työasemalla toimialueeseen (Asetukset > Järjestelmä > Tietoja > Nimeä tämä tietokone uudelleen (lisäasetus) > Järjestelmän ominaisuudet > Muuta…) muuttamalla jäsenyys työryhmästä toimialueeksi amidom.local ja antamalla Tietokoneen nimi ja toimialuemuutokset -kohdassa tietokoneen tilille oikeus kirjautua toimialueelle (Administrator, P@ssw0rd). Käynnistettiin tietokone uudelleen ja kirjauduttiin Administrator-tunnuksella sisään.

Lisättiin palvelimella Physio-organisaatioyksikköön (Server Manager > Tools > Active Directory Users and Computers) Työasemat no updates -yksikkö. Tarkistettiin palvelimella (Server Manager > Tools > DHCP > server1.amidom.local > IPv4 > Scope [192.168.100.0] Wks > Address Leases), että wks2 löytyy listasta wks1:n lisäksi. Siirrettiin wks2 Työasemat no updates -yksikköön (Server Manager > Tools > Active Directory Users and Computers) ja käynnistettiin se uudelleen.

Asennettiin Wireshark 4.4.3 työasemalle (Wireshark Foundation, Download Wireshark, 2025). Testattiin toimivuus ja tallennettiin capture (wireshark_capture_19022025). Sammutettiin palvelin ja työasema sekä otettiin snapshot 20250219 työasemasta ja varmuuskopioitiin se ulkoiselle kovalevylle.

Kali Linux-virtuaalikone on ladattu aiemmin valmiina (OffSec Services Limited, 2025).

Lisäksi Hack the Box -verkkosivustosta tehtiin Nmap-aiheista osuutta (Hack the Box, 2025) Parrot Linux-koneella VMWaressa.

2.1 Physio-websovellus virtuaalikoneeseen

Palvelin ja työasema käynnistettiin. Physio-websovellus käynnistettiin wks2-työasemassa ChatGPT:n avulla:

- Työasemaan ladattiin Node.js v22.14.0 ja npm (Foundation, 2025)
- Asennettiin git 2.48.1 (winget install --id Git.Git -e --source winget) ja lisättiin se PATH-muuttujaan (C:\Program Files\Git\bin, C:\Program Files\Git\cmd)
- Kloonattiin physio-web-pages-tietovarasto ilman tiedostojen automaattista tarkistusta (git clone --no-checkout https://github.com/hannahakonen/physio-web-pages.git, cd physio-web-pages, git checkout HEAD --), koska Windows ei tukenut kaikkia tiedostonimiä (":")
- Asennettiin npm Physion kansioon (C:\Users\Administrator\physio-web-pages>npm install)
- Asennettiin cross-env Physion api-kansioon (npm install cross-env)
- Sallittiin Node.js käyttö, koska Windows Defenderin palomuuri esti osan sen ominaisuuksista
- Lisättiin vielä api-kansioon ympäristömuuttujat .env-tiedostoon eli MongoDB Atlaksen osoite ja salasana sekä käytettävä portti 3001)
- Käynnistettiin Physio portissa 3001 api-kansiosta (npm run dev)

3 Verkonvalvontasuunnitelma

Suunnitelmassa kuvataan, miten tietoverkon toimintaa ja tietoturvaa seurataan erilaisilla työkaluilla (OpenAI, 2025). Verkonvalvonnan tavoitteet ovat epäilyttävän tai poikkeavan verkkoliikenteen havaitseminen, palvelinten ja työasemien suorituskyvyn ja lokitietojen valvominen, mahdollisten haavoittuvuuksien tunnistaminen ja niihin ajoissa reagoiminen sekä havaintojen raportoiminen ja toimenpiteiden suositteleminen.

3.1 Poikkeava verkkoliikenne

Poikkeavan verkkoliikenteen havaitseminen, kuten Nmap-skannaukset tai epäilyttävät yhteydet, suoritetaan Wiresharkilla ja Tcpdumpilla (The Tcpdump Group, 2025) Windows-serverissä ja työasemassa. Wireshark on avoimen lähdekoodin verkkoprotokolla-analysaattori ja Tcpdump on komentorivityökalu pakettien sieppaamiseen ja analysointiin.

3.2 Palvelimen ja työaseman tila

Palvelimen ja työaseman tilaa, kuten prosessorin kuormitusta, muistin käyttöä ja verkkoyhteyksiä, tutkitaan Performance Monitorilla, Task Managerilla tai kolmannen osapuolen ohjelmilla kuten Zabbix (Zabbix LLC, 2025). Performance Monitor seuraa verkon suorituskykyä, kuten kaistanleveyden käyttöä, viiveitä tai pakettien pudotuksia.

3.3 Kirjautumiset ja lokit

Kirjautumisia ja lokeja valvotaan Windows Event Viewerillä, System Monitorilla (Sysmon) (Microsoft, Sysmon v15.15, 2025) ja Powershellillä. Windows Event Viewer seuraa ja analysoi verkkoon liittyviä tapahtumalokeja, kuten kirjautumisyrityksiä, verkkoyhteysvirheitä ja tietoturvahälytyksiä.

3.4 Haavoittuvuudet

Windows-palvelimen ja -työaseman avoimia verkkoyhteyksiä skannataan Nmapilla Kali Linux-koneella. Molempien haavoittuvuuksia skannataan Nessus Essentialsilla palvelimella.

3.5 Edistyneemmät valvontatyökalut

Edistyneempiä valvontatyökaluja olisivat SIEM (Security Information and Event Management), kuten Microsoft Sentinel (Microsoft, What is Microsoft Sentinel?, 2025) ja IDS/IPS (Intrusion Detection

System/Intrusion Prevention System), joka on mukana esimerkiksi Azure Firewall Premiumissa (Microsoft, Azure Firewall Premium features, 2025).

Lähdeluettelo

Foundation, O. (1. Maaliskuu 2025). *Run JavaScript Everywhere*. Noudettu osoitteesta https://nodejs.org/

Hack the Box. (25. Helmikuu 2025). *Network Enumeration with Nmap*. Noudettu osoitteesta https://academy.hackthebox.com/module/details/19

Microsoft. (24. Helmikuu 2025). *Azure Firewall Premium features*. Noudettu osoitteesta https://learn.microsoft.com/en-us/azure/firewall/premium-features

Microsoft. (24. Helmikuu 2025). *Sysmon v15.15*. Noudettu osoitteesta https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Microsoft. (24. Helmikuu 2025). *What is Microsoft Sentinel?* Noudettu osoitteesta https://learn.microsoft.com/en-us/azure/sentinel/overview?tabs=azure-portal

OffSec Services Limited. (25. Helmikuu 2025). *Kali*. Noudettu osoitteesta https://www.kali.org/get-kali/#kali-virtual-machines

OpenAI. (24. Helmikuu 2025). *ChatGPT*. Noudettu osoitteesta https://chatgpt.com/

The Tcpdump Group. (18. Helmikuu 2025). *Tcpdump & lipbcap*. Noudettu osoitteesta https://www.tcpdump.org/

Wireshark Foundation. (18. Helmikuu 2025). *Download Wireshark*. Noudettu osoitteesta https://www.wireshark.org/download.html

Wireshark Foundation. (18. Helmikuu 2025). *Wireshark*. Noudettu osoitteesta https://www.wireshark.org/

Zabbix LLC. (24. Helmikuu 2025). *Zabbix*. Noudettu osoitteesta https://www.zabbix.com/