YHTEENVETO HAAVOITTUVUUSSKANNAUKSISTA JA KEHITYS-EHDOTUKSET

Johanna Hakonen

Sisällysluettelo

1 Johdanto

Kyberturvariskejä hallitaan esimerkiksi skannaamalla haavoittuvuuksia erilaisilla ohjelmilla kuten Nmap, Nessus Essentials ja SQLmap. Tässä vertaillaan Nmap- ja Nessus Essentials-skannauksien tuloksia. Nmap-skannaukset on analysoitu erikseen liitteissä 4b ja 4c sekä versioskannauksen tulos on liitteessä 4d. Hack the Box -sivuston Nmap-tehtävät on esitelty liitteessä 5a. Nessus Essentials-skannaukset on analysoitu liitteessä 5b ja raportit on liitteissä 5c-f.

Ympäristönä toimi Windows-palvelin, wks2-työasema VMwaressa ja Kali Linux-kone, ja sen asennus on esitetty liitteissä 4a ja 5b. Physio-websovellus oli käynnissä työaseman portissa 3001.

2 Yhteenveto haavoittuvuusskannauksista

Kali Linux-koneen Nmapilla skannattiin koko ympäristöstä kohteet ja työaseman portteja tarkemmin SYN-, TPC- ja versioskannauksilla. Tehtiin kaksi erillistä sarjaa, Physio-web-sovelluksen kanssa ja ilman. Palvelimeen asennetulla Nessus Essentialsilla skannattiin koko ympäristöstä kohteet ja palvelintakin tarkemmin sekä työasemasta vielä erikseen Physio-web-sovellusta tarkemmin Web Application Tests -skannauksella.

2.1 Kohteet

Nmapilla ja Nessus Essentialsilla löytyi samat kohteet: VMware 192.168.100.1, oletusyhdyskäytävä 192.168.100.2, palvelin 192.168.100.11 ja työasema 192.168.100.100 tai 192.168.100.101. Nmapilla näkyi myös Kali Linux-kone 192.168.100.129, joka ei ollut käynnissä Nessus-skannauksissa.

2.2 Windows-työasema

Nmapilla havaittiin, että työaseman käyttöjärjestelmä on Windows (ttl=128). Nessus löysi käyttöjärjestelmäksi Microsoft Windows 10 tai Microsoft Windows Server 2019.

2.2.1 Portit

Nmapilla tutkittiin työaseman 10 suosituinta porttia (21, 22, 23, 25, 80, 110, 139, 443, 445 ja 3389), joista havaittiin auki olevan 139 ja 445. Physion portin 3001 (HTTP) havaittiin olevan auki myös. Näistä muut skannatut portit olivat filtered-tilassa eli Nmap ei pystynyt määrittämään, onko portti auki vai kiinni. Nessuksella löytyi samat avoimet portit 139, 445 ja 3001 sekä lisäksi 135.

2.2.2 Palvelut

Nmap ilmoitti työaseman portin 139 palvelun olevan Netbios-SSN ja Nessus SMBv2. SMB on palvelimen viestilohko (Server Message Block), joka pyörii Netbios-SSN:n (Session Service) päällä TCP-portissa 139 (Chavan, 2025) eli molemmat ohjelmat kertoivat oikein.

Nmap ilmoitti työaseman portin 445 palvelun olevan Microsoft-DS ja Nessus CIFS. CIFS eli Common Internet File System on SMB:n laajennettu mutta vanhentunut versio (SMBv1) ja nykyään käytetään uudempia SMB-versioita 2.0 ja 3.0 (Informa TechTarge, 2025) kuten Nessuksen mukaan portissa 139. Windowsissa SMB voi pyöriä suoraan TCP-portissa 445 käyttäen Microsoft-DS-palvelua (Chavan, 2025), joten molemmat ohjelmat havaitsevat oikein. Nessus löysi myös keskitason SMB Signing not required -haavoittuvuuden eli kirjautumista ei vaadita SMB-palvelimella, jolloin todentamaton hyökkääjä voi suorittaa man-in-the-middle-hyökkäyksen.

Nmap ilmoitti SYN- ja TCP-skannauksilla työaseman portin 3001 palvelun olevan Nessus mutta versioskannauksella löytyi oikea eli HTTP. Nessus löysi myös HTTP:n.

Nessuksella löytyi DCE/RPC-palvelu seuraavista työaseman porteista: 135 (EPMAP), 49665, 49666, 49667, 49670, 49676 ja 49696.

2.2.3 Muut tiedot

Nessuksella löytyi myös muita tietoja työasemasta, joita ei Nmapilla tutkittu. Koneen nimi löydettiin: WKS2 ja WKS2.amidom.local sekä laitetyyppi ”general-purpose” ja se, että se on VMware-virtuaalikone.

2.2.4 Physio

Nmapin versioskannauksella löydettiin portista 3001 Physio-web-sovelluksessa käytetty Node.js Express -framework, kun taas Nessus ei suoraan ilmoittanut sitä, mutta sillä löytyi kuitenkin tieto asiasta (X-Powered-By: Express). Nessuksella löytyi myös muuta tietoa (HTTP/1.1, SSL: ei, Keep-Alive: kyllä ja ja robot.txt:n sisältö). SSL tulee korjata mutta Keep-Alive ei ole haavoittuvuus mutta voi paljastaa palvelimen käyttäytymistä. Robot.txt-tiedosto voi sisältää arkaluonteista tietoja kuten turvallisuuskriittisiä tiedostopolkuja.

Työasemalle tehtiin lisäksi Physion-websovelluksen vuoksi Web Application Scan -skannaus (192.168.100.100) (liite 5f), jolla saatiin uutta tietoa. Nessus keräsi ulkoiset linkit, jotka liittyivät kaikki Physio-sovelluksen fontteihin. Ne ovat luotettavilta palvelimilta (Google), joten tämä ei ole ongelma. Löydettiin myös eri kansioiden sallitut HTTP-metodit, joista löytyi kaikki muut ei-turvallisiksi katsotut (DELETE, HEAD, PUT, TRACE) kansioissa “/”, “/static” ja “/static/css”, paitsi CONNECT.

Lisäksi Nessus havaitsi, että Physio asettaa joissakin vastauksissa sisällön suojauskäytäntöön (Content-Security-Policy, CSP) liittyvän sallivan frame-ancestors-vastausotsikon (Mozilla, 2025) tai ei aseta sitä ollenkaan, mikä mahdollistaa sivustojen välistä komentosarjahyökkäykset (cross-site scripting, XSS) ja klikkaushyökkäykset (clickjacking). Lisäksi Physio asettaa joissakin vastauksissa sallivan X-Frame-Options -vastausotsikon (Helmet.js, 2025) tai ei aseta sitä ollenkaan. Nämä liittyvät toisiinsa siten, että

X-Frame-Options on vanha otsikko, jonka CSP-direktiivi frame-ancestors on korvannut, mutta jota käytetään vanhemmissa selaimissa.

Nessus pystyi myös käymään läpi linkitettävää sisältöä, jota voidaan käyttää tiedon keräämiseen kohteesta. Luotiin seuraava sivukartta: http://WKS2:3001/, http://WKS2:3001/favicon.ico, http://WKS2:3001/logo192.png, http://WKS2:3001/manifest.json ja http://WKS2:3001/static/css/main.3784df71.css. Nämä saattavat paljastaa meta-tietoa sovelluksesta tai paljastaa käytössä olevan frameworkin.

2.3 Windows-palvelin

Palvelinta tutkittiin vain Nessuksella ja sillä löytyi paljon tietoa palvelimesta. Palvelin on mahdollisesti virtuaalikone, käyttöjärjestelmä on Microsoft Windows ja laitteen tyyppi on ”general-purpose”. Koneen nimi SERVER01 ja Server01.amidom.local, toimialue on AMIDOM, alueen nimi (realm) on AMIDOM.LOCAL ja palvelimen aika 2025-03-08 11:04:17 UTC skannaushetkellä.

Palvelimesta Nessus löysi avoimia portteja yli 1024 (skannattujen porttien maksimi): 53, 88, 123, 135, 139, 389, 443, 445, 464, 593, 636, 3268, 3269, 5353, 5355, 5985, 8834, 9389, 47001, 49664, 49665, 49670… 65423.

Palvelimesta havaittiin eri palveluja: DNS (TCP-portti 53), NTP (123), SMBv2 (139), LDAP (389), CIFS (445), HTTP-RPC-EPMAP (593), LDAP (3268) ja NCACN_HTTP (49670).

Web-palvelimia löytyi useampi: 443 (HTTPS), 5985, 8834 (Nessus, TLSv1.2) ja 47001. Porteista 5985 ja 47001 saatiin tiedot: HTTP/1.1, SSL: ei ja Keep-Alive: ei.

Portista 443 saatiin myös lisätietoja: salausversiot (TLSv1.1, TLSv1.2, TLSv1.3), SSL-sertifikaatti saadaan näkyviin, HTTP/1.1 ja Keep-Alive: ei.

Portista 443 löytyi korkean tason SSL Medium Strength Cipher Suites Supported (SWEET32) -haavoittuvuus eli palvelin tukee keskivahvaa SSL-salausta, jossa avaimen pituus on 64 ja 112 bitin välillä tai 3DES-salausta.

Portista 443 löytyi myös keskitason haavoittuvuuksia. Portin Windows Admin Centeriin liittyvä sertifikaatti on vanhentunut ja sen on allekirjoittanut tuntematon sertifikaattiviranomainen (Windows Admin Center Root CA). Lisäksi SSL-sertifikaatin 'commonName' (CN) -attribuutit Windows Admin Center ja WIN-TJ57E46KUM3 ovat eri kuin Nessuksen tunnistamat server01 ja Server01.amidom.local. X.509-sertifikaatti ei siis ole luotettava ja luottamusketju voi olla rikki. Jos palvelin olisi tuotannossa, jokainen ketjun katkeaminen vaikeuttaa verkkopalvelimen aitouden ja identiteetin varmistamista. Tämä saattaa helpottaa man-in-the-middle-hyökkäysten suorittamista kohdetta vastaan.

Lisäksi portin 443 palvelussa on keskitason haavoittuvuutena käytössä vanhat TSL 1.0 - ja 1.1 -versiot, joissa on useita kryptografisia suunnitteluvirheitä ja niistä puuttuu tuki nykyisille ja suositelluille salaussarjoille. Niiden kanssa ei voida käyttää salauksia, jotka tukevat salausta ennen MAC-laskentaa, eikä todennettuja salaustapoja kuten GCM, eivätkä ne toimi enää kunnolla internetselainten kanssa.

Portin 443 palvelussa ei myöskään ole käytössä HTTP Strict Transport Securitya (HSTS), joka pakottaisi selaimen käyttämään vain HTTPS-protokollaa. Tämä altistaa downgrade- ja SSL-stripping man-in-the-middle -hyökkäyksille sekä heikentää keksinkaappaussuojaa.

DCE/RPC-palvelu löytyi seuraavista porteista: 135 (EPMAP), 445 (CIFS), 49664, 49665, 49666, 49667, 49668, 65386, 65389, 65393, 65395, 65407 ja 65423.

3 Kehitysehdotukset

Tässä esitetään kehitysehdotuksia haavoittuvuusskannausten pohjalta. Palvelimen TCP-portissa 443 on useita haavoittuvuuksia, jotka tulisi hoitaa ensimmäisenä. Työasemana käytettiin viimeksi vuonna 2023 päivitettyä virtuaalikonetta, jonka päivittäminen saattaa ratkaista löydettyjä haavoittuvuuksia. NoSQL-tietokannan injektiohaavoittuvuuksia tulisi tutkia Medusalla tai Burp Suitella.

3.1 Palvelimen portti 443

Korkean tason SSL Medium Strength Cipher Suites Supported (SWEET32) -haavoittuvuus TCP-portissa 443 (HTTPS) eli keskivahvan SSL-salauksen tukeminen (avaimen pituus on 64 ja 112 bitin välillä tai 3DES-salaus) tulee hoitaa eli tukea vahvaa salausta.

Palvelimen portin 443 vanhentuneeseen ja väärään SSL-sertifikaattiin liittyvät keskitason haavoittuvuudet hoidetaan oikean SSL-sertifikaatin ostamisella tai luonnilla.

Lisäksi portin 443 palvelussa käytössä olevien vanhojen versioiden TSL 1.0 ja 1.1 tuki tulee poistaa (keskitason haavoittuvuus) ja ottaa käyttöön tuki TLS 1.2:lle ja/tai 1.3:lle.

Palvelimen portin 443 palveluun tulee ottaa HTTP Strict Transport Security (HSTS) -asetus käyttöön, joka pakottaa selaimen käyttämään vain HTTPS-protokollaa.

3.2 Työaseman portti 445

Työasemalta löytynyt TCP-portin 445 keskitason SMB Signing not required -haavoittuvuus hoidetaan pakottamalla kirjautuminen asetuksissa. Windowsissa se tehdään policy-asetuksessa “Microsoft network server: Digitally sign communications (always)”.

Tulee varmistaa, ettei CIFS (SMBv1) ole käytössä, koska tällöin kirjautumista ei voi pakottaa. ChatGPT ehdottaa tarkistusta Nmapilla (nmap --script smb-protocols -p 445 <kohde-IP> tai Powershellillä (Get-WindowsFeature FS-SMB1, Disable-WindowsOptionalFeature -Online -FeatureName "SMB1Protocol" -NoRestart).

3.3 Työaseman Physio

3.3.1 X-powered-By

Nmapin versioskannauksella löydettiin portista 3001 Physio-websovelluksessa käytetty Node.js Express framework, kun taas Nessus ei suoraan ilmoittanut sitä, mutta sillä löytyi kuitenkin tieto asiasta (”X-Powered-By: Express”). Tähän on ratkaisuna käyttää Helmet.js-väliohjelmistoa, joka suojaa Express-pohjaisia sovelluksia asettamalla http-otsikoita oikein (OpenJS Foundation, 2025). X-powered-By saadaan ottaa pois käytöstä myös komennolla ”app.disable('x-powered-by')”. Näin saatu suoja ei ole täydellinen mutta estää yksinkertaiset hyökkäykset.

3.3.2 HTTP-metodit

Löydettiin myös eri kansioiden sallitut HTTP-metodit, joista löytyi kaikki muut ei-turvallisiksi katsotut (DELETE, HEAD, PUT, TRACE) kansioissa “/”, “/static” ja “/static/css”, paitsi CONNECT. ChatGPT ehdottaa ratkaisuksi Expressin kanssa lisätä seuraava koodi server.js- tai app.js-tiedostoon:

```
const express = require('express');
const app = express();

// Estetään ei-toivotut HTTP-metodit
const allowedMethods = ['GET', 'POST'];
app.use((req, res, next) => {
  if (!allowedMethods.includes(req.method)) {
    return res.status(405).send('Method Not Allowed');
  }
  next();
});

// Muu palvelinlogiikka...
```

3.3.3 X-Frame-Options/frame-ancestors

Sallivaan X-Frame-Options-otsikkoon ratkaisu on asetus ”deny” (Helmet.js, 2025):

```
// Sets "X-Frame-Options: DENY"
app.use(
 helmet({
  xFrameOptions: { action: "deny" },
 }),
);
```

Ja sallivaan frame-ancestors-otsikkoon ratkaisu on asetus ”none” (Mozilla, 2025):

```
HTTP: Content-Security-Policy: frame-ancestors 'none';
```

Tulee selvittää, täytyykö molemmat asettaa samaan aikaan.

3.3.4 Muut

HTTPS tulee pakottaa lisäämällä koodiin (Stack Exchange Inc, 2025):

```
app.enable('trust proxy')
app.use((req, res, next) => {
 req.secure ? next() : res.redirect('https://' + req.headers.host + req.url)
})
```

Nessuksen löytämän robots.txt-tiedoston sisältö tulee tarkistaa. Nessus ehdottaa Robots-Meta-tagien käyttämistä sen sijasta tai säätämään palvelun käyttöoikeuksien valvonta rajoittamaan pääsyä materiaaleihin. Löydetyistä sivukartan tiedostoista kannattaa ChatGPT:n mukaan tarkistaa manifest.json, ettei se paljasta liikaa tietoa kuten versiotietoja tai sisäisiä URL-osoitteita. Bottien pääsyä tiettyihin tiedostoihin voi estää robot.txt:llä tai määrittämällä CSP (Content-Security-Policy: default-src 'self';).

Lähdeluettelo

Chavan, Y. (13. Maaliskuu 2025). *Medium*. Noudettu osoitteesta Difference Between NetBIOS & SMB: https://medium.com/@chavanyashwardhan/difference-between-netbios-smb-1cd74ec02fdd

Helmet.js. (14. Maaliskuu 2025). *Helmet.js*. Noudettu osoitteesta https://helmetjs.github.io/

Informa TechTarge. (13. Maaliskuu 2025). *Common Internet File System (CIFS)*. Noudettu osoitteesta https://www.techtarget.com/searchstorage/definition/Common-Internet-File-System-CIFS

Mozilla. (14. Maaliskuu 2025). *CSP: frame-ancestors*. Noudettu osoitteesta https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Content-Security-Policy/frame-ancestors

OpenJS Foundation. (14. Maaliskuu 2025). *Security Best Practices for Express in Production*. Noudettu osoitteesta https://expressjs.com/en/advanced/best-practice-security.html

Stack Exchange Inc. (15. Maaliskuu 2025). *Stack Overflow*. Noudettu osoitteesta Automatic HTTPS connection/redirect with node.js/express: https://stackoverflow.com/questions/7450940/automatic-https-connection-redirect-with-node-js-express