HAAVOITTUVUUKSIEN SKANNAUS: CASE-ESIMERKKI NESSUS ESSENTIALS

Johanna Hakonen

Sisällysluettelo

1 Johdanto

Kyberturvariskejä hallitaan esimerkiksi skannaamalla haavoittuvuuksia erilaisilla ohjelmilla kuten Nmap, Nessus Essentials ja Openvas. Tässä esitellään skannaukset Nessus Essentialsilla.

Ympäristönä toimi Windows-palvelin ja wks2-työasema VMwaressa ja sen asennus on esitetty liitteessä 4a. Physio-websovellus oli käynnissä työaseman portissa 3001.

2 Nessus Essentials

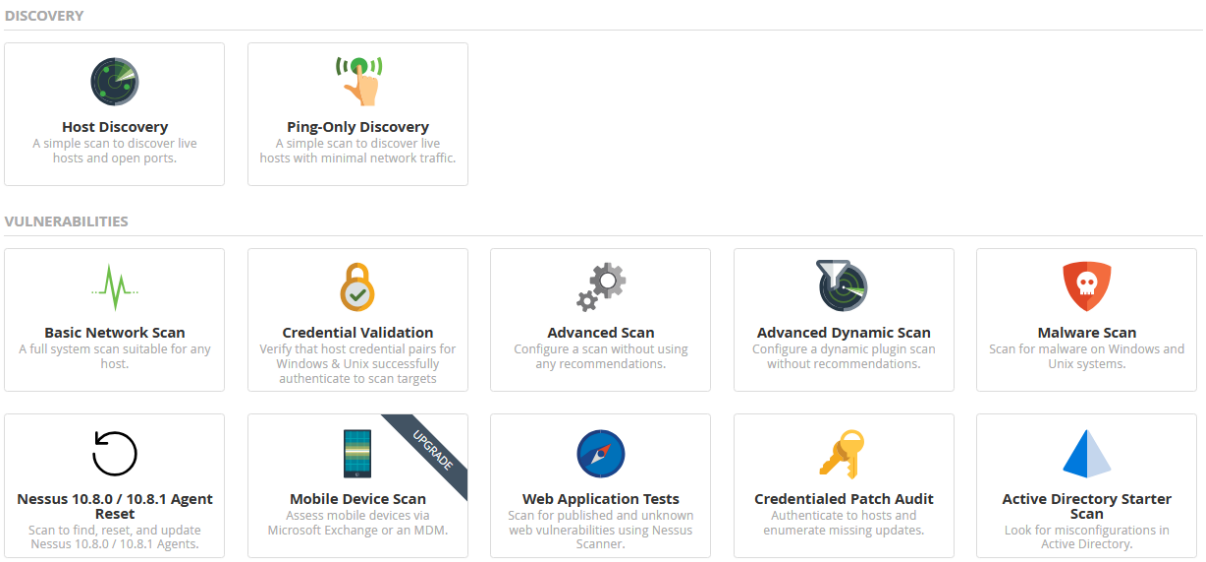
2.1 Asennus Windows-palvelimelle

Käynnistettiin palvelin ja tehtiin Windows Updaten ehdottamat päivitykset: Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.270.0) ja Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.25010.11).

Ladattiin Nessus Essentials (Tenable, Inc., Tenable nessus essentials vulnerability scanner, 2025) ja asennettiin se. Ohjelma aukesi sivulle http://localhost:8834/WelcomeToNessus-Install/welcome, klikattiin ”Connect via SSL”. Ei muutettu asetuksia alussa ja valittiin ”Register for Nessus Essentials”. Käytettiin aktivointikoodia, joka saatiin ennen latausta, ja luotiin käyttäjätili. Nessus ilmoitti, että palvelimen muisti ei riitä, joten sammutettiin se, otettiin snapshot 20250308 ja backup ulkoiselle kovalevylle. Lisättiin muistia neljästä GB:stä kuuteen ja pluginien asennus onnistui.

2.2 Skannaukset

Tehtiin koko IP-alueelle (192.168.100.0/24) Host Discovery -, Ping-Only Discovery - ja Basic Network Scan -skannaukset. Työasemaan tehtiin lisäksi Web Application Tests -skannaus. Kuva 1 on esitetty osa Nessus Essentialsin skannausvaihtoehdoista. Haavoittuvuuksille ohjelma antaa viisi eri vakavuustasoa: kriittinen, korkea, keskitaso, matala ja info. Eri haavoittuvuuksien havaitsemisohjelmia sanotaan laajennuksiksi (plugin) (Tenable, Inc., Tenable Plugins, 2025). Tässä ei käsitellä VMware-ympäristöön (192.168.100.1, 192.168.100.2) liittyviä haavoittuvuuksia. Lopussa suljettiin serveri, otettiin snapshot 20250308_2 ja varmuuskopioitiin ulkoiselle kovalevylle.



Kuva 1. Osa Nessus Essentialsin skannausmahdollisuuksista.

3 Discovery-skannaukset

3.1 Host Discovery

Host Discovery -skannauksella (192.168.100.0/24) (liite 5c) löytyi laitteet ja avoimet portit:

Host	FQDN	Ports
192.168.100.100		135, 139, 445, 49664, 49665, 49666, 49667, 49670, ...
192.168.100.11	Server01.amidom.local	135, 139, 389, 445, 3268, 49664, 49665, 49666, 496...
192.168.100.2		
192.168.100.1		135, 49664, 49665, 49666, 49667, 49668, 49675

Tuloksena saatiin käytössä olevat IP-osoitteet: VMware 192.168.100.1, oletusyhdyskäytävä 192.168.100.2, palvelin 192.168.100.11, työasema 192.168.100.100. Portit eivät näy raportissa vaan ainoastaan ohjelman käyttöliittymässä, mutta ne löytyvät Basic Network Scan -skannauksen raportista (liite 5e) ja käsitellään myöhemmin.

Host Discovery-skannauksella löytyi kaksi info-tason haavoittuvuutta jokaiselle kohteelle:

Sev	CVSS	VPR	EPSS	Name	Family	Count
INFO				Nessus Scan Information	Settings	4
INFO				Ping the remote host	Port scanners	4

Nessus Scan Information -plugin kertoo tietoa skannauksesta itsestään (Tenable, Inc., Tenable Nessus Scan Information, 2025). Ping the Remote Host -plugin kertoo, että oli mahdollista selvittää, onko skannattava kohde ylhäällä (Tenable, Inc., Tenable Ping the remote host, 2025).

3.2 Ping-Only Discovery -skannaus

Ping-Only Discovery -skannauksella (192.168.100.0/24) (liite 5d) saatiin samat info-tason haavoittuvuudet kuin edellisessä kohdassa, koska niissä molemmissa käytettiin Ping the Remote Host-pluginia:

Host	Vulnerabilities
192.168.100.1	2
192.168.100.2	2
192.168.100.11	2
192.168.100.100	2

Sev	CVSS	VPR	EPSS	Name	Family	Count
INFO				Nessus Scan Information	Settings	4
INFO				Ping the remote host	Port scanners	4

4 Vulnerabilities-skannaukset

4.1 Basic Network Scan

Basic Network Scan -skannauksella (192.168.100.0/24) (liite 5e) löytyi yksi korkean tason, kahdeksan keskitason ja yli tuhat info-tason haavoittuvuutta, joista 1024 (skannattujen porttien maksimi) oli Netstat Portscanner (SSH) -ohjelman löytämiä avoimia portteja palvelimessa:

Host	Vulnerabilities
192.168.100.11	1101
192.168.100.100	35
192.168.100.1	16
192.168.100.2	2 13

Sev	CVSS	VPR	EPSS	Name	Family	Count
MIXED	...	...	...	9 SSL (Multiple Issues)	General	13
MEDIUM	6.5	4.0	0.0035	IP Forwarding Enabled	Firewalls	1
MEDIUM	5.3			SMB Signing not required	Misc.	1
MIXED	...	...	...	5 TLS (Multiple Issues)	Service detection	7
MIXED	...	...	...	3 DNS (Multiple Issues)	DNS	5
INFO	...	...	...	6 SMB (Multiple Issues)	Windows	13
INFO	...	...	...	3 HTTP (Multiple Issues)	Web Servers	7
INFO	...	...	...	2 Microsoft Windows (...	Windows	3
INFO	...	...	...	2 TLS (Multiple Issues)	General	3
INFO				Netstat Portscanner (SSH)	Port scanners	1024
INFO				DCE Services Enumeration	Windows	30

INFO	Service Detection	Service detection	9	
INFO	Nessus SYN scanner	Port scanners	7	
INFO	Common Platform Enumer...	General	4	
INFO	Device Type	General	4	
INFO	Nessus Scan Information	Settings	4	
INFO	OS Fingerprints Detected	General	4	
INFO	OS Identification	General	4	
INFO	Traceroute Information	General	3	
INFO	Ethernet Card Manufactur...	Misc.	2	
INFO	Ethernet MAC Addresses	General	2	
INFO	Host Fully Qualified Domai...	General	2	
INFO	LDAP Crafted Search Requ...	Misc.	2	
INFO	LDAP Server Detection	Service detection	2	
INFO	OS Security Patch Assessm...	Settings	2	
INFO	Service Detection (HELP Re...	Service detection	2	
INFO	Target Credential Status by...	Settings	2	
INFO	VMware Virtual Machine D...	General	2	
INFO	Additional DNS Hostnames	General	1	
INFO	Kerberos Information Discl...	Misc.	1	
INFO	Nessus Server Detection	Service detection	1	
INFO	Nessus Windows Scan Not ...	Settings	1	
INFO	Netstat Connection Inform...	General	1	
INFO	Network Time Protocol (NT...	Service detection	1	
INFO	OS Identification and Instal...	Misc.	1	
INFO	Strict Transport Security (S...	Service detection	1	
INFO	TLS ALPN Supported Proto...	Misc.	1	
INFO	Web Server robots.txt Infor...	Web Servers	1	
INFO	WS-Management Server D...	Web Servers	1	

Scan Notes ▲

Portscanner Max Ports Exceeded
Warning: portscanners have found more than 1024 ports open for target 192.168.100.11, and the number of reported ports has been truncated to 1024 (threshold controlled by scanner preference portscanner.max_ports). Usually this is due to intervening network equipment intercepting and responding to connection requests as a countermeasure against portscanning or other potentially malicious activity. Since this negatively impacts both scan accuracy and performance, you may want to adjust your network security configuration to disable this behavior for vulnerability scans.

4.1.1 Palvelimen haavoittuvuudet

Yhteenveto palvelimen haavoittuvuuksista:

192.168.100.11

0	1	6	0	1101
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Sat Mar 8 13:02:42 2025
End time:	Sat Mar 8 13:18:30 2025

Host Information

DNS Name:	Server01.amidom.local
Netbios Name:	SERVER01
IP:	192.168.100.11
OS:	Windows

Palvelimesta löytyi korkean tason SSL Medium Strength Cipher Suites Supported (SWEET32) -haavoittuvuus tcp-portista 443 (www) eli palvelin tukee keskivahvaa SSL-salausta, jossa avaimen pituus on 64 ja 112 bitin välillä tai 3DES-salausta. Jos hyökkääjä on samassa fyysisessä verkossa, on paljon helpompaa kiertää keskivahvaa salausta. Ratkaisuna Nessus ehdottaa keskivahvan salauksen välttämistä, jos vain mahdollista.

Palvelimesta löytyi vanhentuneeseen ja väärään SSL-sertifikaattiin liittyvät keskitason haavoittuvuudet sekä vanhaan TLS-versioon liittyvä keskitason haavoittuvuus, jotka on esitelty alla.

4.1.1.1 SSL Certificate Cannot Be Trusted

Palvelimesta löytyi kaksi keskitason SSL Certificate Cannot Be Trusted -haavoittuvuutta. TCP-portissa 443 (www) Windows Admin Centeriin liittyvä sertifikaatti (sertifikaattiketjun osa) on vanhentunut. Lisäksi siihen liittyvän sertifikaatin (sertifikaattiketjun päällimmäinen) on allekirjoittanut tuntematon sertifikaattiviranomainen (Windows Admin Center Root CA).

TCP-portissa 8834 (www) Nessukseen liittyvän sertifikaatin (sertifikaattiketjun päällimmäinen) on allekirjoittanut tuntematon sertifikaattiviranomainen (Nessus Users United/Nessus Certification Authority).

Haavoittuvuuden kuvauksessa sanotaan, että palvelimen X.509-sertifikaatti ei 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. Ratkaisuksi Nessus ilmoittaa kunnollisen SSL-sertifikaatin ostamista tai luomista.

4.1.1.2 SSL Certificate Expiry

Tämä keskitason haavoittuvuus viittaa samaan SSL-sertifikaatin vanhentumiseen kuin edellisessä kohdassa: TCP-portin 443 (www) Windows Admin Centeriin liittyvään sertifikaattiin, jonka antaja on Windows Admin Center Root CA. Ohjelma tutkii viimeiset voimassaolopäivät. Ratkaisuksi Nessus ilmoittaa uuden SSL-sertifikaatin ostamista tai luomista.

4.1.1.3 SSL Certificate with Wrong Hostname

Tämä keskitason haavoittuvuus viittaa edelleen samaan TCP-portin 443 (www) Windows Admin Centeriin liittyvään SSL-sertifikaattiin. SSL-sertifikaatin 'commonName' (CN) -attribuutit Windows Admin Center ja WIN-TJ57E46KUM3 ovat eri kuin Nessuksen tunnistamat server01 ja Server01.amidom.local. Ratkaisuksi Nessus ilmoittaa kunnollisen SSL-sertifikaatin ostamista tai luomista.

4.1.1.4 TLS Version 1.0 Protocol Detection

Palvelimen TCP-portin 443 (www) palvelu salaa liikenteen käyttämällä vanhaa versiota TLS 1.0 (keskitason haavoittuvuus) ja palvelin tukee ainakin yhtä salausta. Kuvauksessa sanotaan, että TLS 1.0:ssa on useita kryptografisia suunnitteluvirheitä ja uudempia versioita 1.2 ja 1.3 tulisi käyttää aina kuin mahdollista. Päätepisteet, jotka eivät käytä näitä, eivät toimi enää kunnolla internetselainten kanssa. PCI DSS v3.2 vaatii, että TLS 1.0 poistetaan kokonaan käytöstä lukuun ottamatta POS/POI-päätteitä.

4.1.1.5 TLS Version 1.1 Deprecated Protocol

Tämä viittaa samaan keskitason haavoittuvuuteen kuin edellinen mutta sanoo, että käytössä on vanha versio TLS 1.1 ja palvelin tukee ainakin yhtä salausta. Kuvauksessa sanotaan, että palvelun hyväksymältä TLS 1.1-salaukselta puuttuu tuki nykyisille ja suositelluille salaussarjoille. Sen kanssa ei voida käyttää salauksia, jotka tukevat salausta ennen MAC-laskentaa, eikä todennettuja salaustapoja kuten GCM. Ratkaisuksi Nessus ehdottaa TSL 1.1:n tuen poistamisen ja TLS 1.2:n ja/tai 1.3:n tuen käyttöönoton.

4.1.1.6 Info-tason haavoittuvuudet

Nessuksella 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.

Avoimia portteja löytyi yli 1024 (skannattujen porttien maksimi) Netstat Portscanner (SSH) -ohjelmalla: 53, 88, 123, 135, 139, 389, 443, 445, 464, 593, 636, 3268, 3269, 5353, 5355, 5985, 8834, 9389, 47001, 49664, 49665, 49670… 65423. Portit 53, 135 ja 2968 löytyivät myös SYN-skannauksella.

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.

HTTPS-portilla 443 ei 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 cookienkaappaussuojaa. Nessus suosittelee ottamaan HSTS-asetuksen käyttöön.

HTTPS-portista 443 saatiin myös muita tietoja: salausversiot (TLSv1.1, TLSv1.2, TLSv1.3), SSL-sertifikaatti näkyy, HTTP/1.1 ja Keep-Alive: ei.

Porteista 5985 ja 47001 saatiin tiedot: HTTP/1.1, SSL: ei ja Keep-Alive: ei.

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

4.1.2 Työaseman haavoittuvuudet

Yhteenveto työaseman haavoittuvuuksista:

192.168.100.100

0	0	1	0	35
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Sat Mar 8 13:03:17 2025
End time:	Sat Mar 8 13:17:35 2025

Host Information

Netbios Name:	WKS2
IP:	192.168.100.100
MAC Address:	00:0C:29:CF:4C:24
OS:	Microsoft Windows 10 Enterprise, Microsoft Windows Server 2019 LTSC, Microsoft Windows Server 2019

Työasemalta löytyi keskitason SMB Signing not required -haavoittuvuus TCP-portista 445 (CIFS). Kirjautumista ei vaadita SMB-palvelimella, jolloin todentamaton hyökkääjä voi suorittaa man-in-the-middle-hyökkäyksen. Ratkaisuna Nessus ehdottaa kirjautumisen pakottamista asetuksissa. Windowsissa se tehdään policy-asetuksessa “Microsoft network server: Digitally sign communications (always)”.

4.1.2.1 Info-tason haavoittuvuudet

Työasemasta löytyi käyttöjärjestelmä Microsoft Windows 10 tai Microsoft Windows Server 2019, koneen nimi WKS2 ja WKS2.amidom.local sekä laitetyyppi ”general-purpose”. VMware löytyi Ethernet-kortin MAC-osoitteen perusteella.

Avoimia portteja löytyi SYN-skannauksella: 135, 139, 445 ja 3001.

Työasemasta havaittiin palveluja: SMBv2 (139) ja CIFS (445).

Webpalvelu (Physio) löytyi portista 3001 ja sen tiedoista HTTP/1.1, SSL: ei, Keep-Alive: kyllä ja X-Powered-By: Express ja robot.txt:n sisältö.

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

4.1.2.2 Web Application Tests

Työasemalle tehtiin lisäksi Physion-websovelluksen vuoksi Web Application Scan -skannaus (192.168.100.100) (liite 5f). Info-tason haavoittuvuudet liittyivät Physio-websovelluksen porttiin 3001. Yhteenveto haavoittuvuuksista:

Host	Vulnerabilities
192.168.100.100	12

Sev	CVSS	VPR	EPSS	Name	Family	Count
INFO	...	...	...	HTTP (Multiple Issues)	CGI abuses	2
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	2
INFO				Nessus SYN scanner	Port scanners	4
INFO				External URLs	Web Servers	1
INFO				Nessus Scan Information	Settings	1
INFO				Web Application Sitemap	Web Servers	1
INFO				Web Server robots.txt Infor...	Web Servers	1

Osa haavoittuvuuksista sisältyi myös Basic Network Scan -skannaukseen. Samat avoimet portit löytyivät SYN-skannauksella: 135, 139, 445 ja 3001. Webpalvelu (Physio) löytyi portista 3001 ja sen tiedoista HTTP/1.1, SSL: ei, Keep-Alive: kyllä ja X-Powered-By: Express ja robot.txt:n sisältö.

Uutta tietoa saatiin myös. Nessus keräsi ulkoiset linkit, jotka liittyivät kaikki Physio-sovelluksen fontteihin.

Löydettiin myös eri kansioiden sallitut HTTP-metodit: ACL, CHECKOUT, COPY, DELETE, GET, HEAD, LOCK, MERGE, MKACTIVITY, MKCOL, MOVE, NOTIFY, OPTIONS, PATCH, POST, PROPFIND, PROPPATCH, PUT, REPORT, SEARCH, SUBSCRIBE, TRACE, UNLOCK ja UNSUBSCRIBE sallittiin kansioissa “/”, “/static” ja “/static/css”. Seuraavat metodit eivät ole turvallisia: PUT, DELETE, CONNECT, TRACE ja HEAD.

Verkkopalvelu ei pyri vähentämään sovelluksen haavoittuvuuksia vaan asettaa joissakin vastauksissa sisällön suojauskäytännön (Content-Security-Policy, CSP) liittyvän sallivan frame-ancestors-vastausotsikon tai ei aseta sitä ollenkaan. W3C:n Web-sovellusten suojaustyöryhmä (Web Application Security Working Group) on ehdottanut CSP:n tavaksi vähentää sivustojen välistä komentosarjahyökkäyksiä (cross-site scripting, XSS) ja klikkaushyökkäyksiä (clickjacking). Nessus suosittelee ei-sallivaa otsikkoa kaikkiin pyydettyihin resursseihin.

Verkkopalvelu asettaa joissakin vastauksissa sallivan X-Frame-Options -vastausotsikon tai ei aseta sitä ollenkaan. Microsoft on ehdottanut X-Frame-Options-otsikon tavaksi vähentää clickjacking-hyökkäyksiä ja tällä hetkellä kaikki suurimmat verkkoselaimet tukevat sitä. Eli ratkaisuksi suositellaan oikein konfiguroitua otsikkoa kaikkiin pyydettyihin resursseihin.

Nessus pystyi 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
- http://WKS2:3001/static/css/main.3784df71.css

Lähdeluettelo

Tenable, Inc. (7. Maaliskuu 2025). *Tenable nessus essentials vulnerability scanner*. Noudettu osoitteesta https://www.tenable.com/products/nessus/nessus-essentials

Tenable, Inc. (10. Maaliskuu 2025). *Tenable Nessus Scan Information*. Noudettu osoitteesta https://www.tenable.com/plugins/nessus/19506

Tenable, Inc. (10. Maaliskuu 2025). *Tenable Ping the remote host*. Noudettu osoitteesta https://www.tenable.com/plugins/nessus/10180

Tenable, Inc. (10. Maaliskuu 2025). *Tenable Plugins*. Noudettu osoitteesta https://www.tenable.com/plugins