

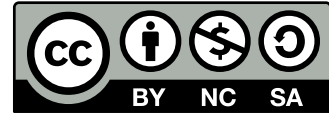
Master's Programme in Computer, Communication and Information Sciences

Hyökkäyspinnan kartoittaminen

Antton Kortelainen

© 2024.

Tämä teos on lisensoitu [Creative Commons](#) “Nimeä-EiKaupallinen-JaaSamoin 4.0 Kansainvälinen” -
käyttöluvalla.



Tekijä Antton Kortelainen

Työn nimi Hyökkäyspinnan kartoittaminen

Koulutusohjelma Master's Programme in Computer, Communication and
Information Sciences

Pääaine Security and Cloud Computing

Työn valvoja Prof. Tuomas Aura

Työn ohjaaja FM Karoliina Kempainen

Päivämäärä 17.4.2024

Sivumäärä 50

Kieli suomi

Tiivistelmä

Internetiin liitettävien laitteiden määrän kasvaessa on tietoverkkojen turvallisuuden ja tiedon eheyden varmistamisesta tullut tärkeää. Hyökkäyspinnan kartoituksessa selvitetään järjestelmien ja tietoverkkojen mahdolliset haavoittuvat kohdat. Havaitsemalla ongelmakohdat ajoissa on organisaation mahdollista korjata ne ennen kuin hyökkääjä pystyy hyväksikäyttämään niitä.

Tässä tutkimuksessa selvitetään, miten järjestelmien haavoittuvia kohtia voi kartoittaa ja miten niiden riskiä voi pienentää. Työssä tarkastellaan olemassa olevia mittareita ja viitekehyksiä järjestelmän tietoturvalle. Työssä käydään läpi työkaluja, joita voi käyttää organisaation järjestelmien hyökkäyspinnan kartoittamiseen. Lisäksi työ esittelee tapoja minimoida järjestelmän hyökkäyspintaa. Tutkimuksessa läpikäytyjen riskien sekä hyökkäyspinnan dynaamisuuden vuoksi tutkimuksessa todetaan hyväksi tavaksi kartoittaa järjestelmiä jatkuvasti, sillä tuntemalla järjestelmät voidaan haavoittuvuuksien riskiä pienentää ja parantaa näin organisaation tietoturvallisuutta.

Tämä tutkimus auttaa organisaatioita kehittämään kattavan mallin hyökkäyspinnan kartoittamiselle sekä tarjoaa näkemyksiä ja suosituksia organisaatioille, jotka haluavat vahvistaa kyberturvallisuuttaan. Tämä tutkimus pyrkii kasvattamaan tietämystä hyökkäyspinnan kartoituksesta ennakoivana strategiana kyberturvallisuuden parantamisessa yhä verkottuneemmassa maailmassa.

Avainsanat tietoturva, hyökkäyspinta, skannaus, tietoverkot

Author Antton Kortelainen

Title Mapping attack surface

Degree programme Master's Programme in Computer, Communication and
Information Sciences

Major Security and Cloud Computing

Supervisor Prof. Tuomas Aura

Advisor Karoliina Kemppainen, M.Sc.

Date 17 April 2024

Number of pages 50

Language Finnish

Abstract

With the increasing number of devices connected to the Internet, ensuring the security and integrity of data networks has become important. The attack surface mapping process identifies potential vulnerabilities in systems and networks. By detecting problems early, an organisation can fix them before an attacker can exploit them.

This study explores how to identify vulnerabilities in systems and how to reduce their risk. It examines existing metrics and frameworks for system security. The study discusses tools that can be used to map the attack surface of an organisation's systems. It also presents ways to minimise the attack surface of a system. Due to the risks discussed in the study and the dynamic nature of the attack surface, the study identifies a good practice to continuously map systems. By knowing the system, risk of vulnerabilities can be reduced, thus improving the security of the organisation.

This study helps organisations develop a comprehensive model for mapping its attack surface and provides insights and recommendations for organisations looking to strengthen their cyber security. This study aims to increase knowledge about attack surface mapping as a proactive strategy for improving cyber security in an increasingly networked world.

Keywords information security, attack surface, scanning, networks

Esipuhe

Haluan kiittää Professori Tuomas Auraa ja ohjaajaani Karoliina Kempaista neuvoista ja ohjauksesta. Lisäksi haluan kiittää myös muita kollegoitani Kyberturvallisuuskeskuksessa neuvoista ja palautteesta.

Helsinki, 17.4.2024

Antton Kortelainen

Sisällysluettelo

Tiivistelmä	3
Tiivistelmä (englanniksi)	4
Esipuhe	5
Sisällysluettelo	6
Käytetyt symbolit ja lyhenteet	8
1 Johdanto	9
2 Tausta	11
2.1 Hyökkäyspinta	12
2.2 Terminologiaa	12
3 Haavoittuvuusmetriikat	14
3.1 CVSS haavoittuvuuksien pisteytykseen	14
3.1.1 CVSS-hyökkäysvektorit	14
3.1.2 CPE järjestelmien yksilöintiin	15
3.2 Hyökättävyys	16
4 Hyökkäyspinnan kartoitus	17
4.1 Porttiskannaus	17
4.1.1 Aktiivinen skannaus	18
4.1.2 Passiivinen skannaus	18
4.1.3 Häiritsevä skannaus	18
4.2 Työkaluja skannaamiseen	19
4.2.1 Nmap	19
4.2.2 Masscan	20
4.2.3 ZMap	20
4.2.4 ZGrab	20
4.3 UDP-porttien skannaus	21
4.4 IPv6-osoitteiden skannaus	22
4.5 Yleisimmin skannatut portit	22
4.6 Verkkotunnusten listaus ja luettelointi	23
4.6.1 Varmenteiden läpinäkyvyys	25
5 Hakukoneet	26
5.1 Esineiden internetin hakukone Shodan	26
5.2 Hyökkäyspinnan kartoittaja Censys	27
5.3 BinaryEdge-palvelu	27
5.4 Hakukoneiden vertailu	28

6	Testiverkon skannaus	29
7	Vastakeinot tietoverkon kartoitukseen	31
7.1	Palomuurit	31
7.1.1	Paketteja suodattavat palomuurit ja tilaton palomuuuri	31
7.1.2	Tilallinen palomuuuri	31
7.1.3	Sovelluspalomuuuri	32
7.1.4	Kehittyneemmät palomuurit	33
7.1.5	Lokitus	34
7.1.6	Palomuurit organisaatioissa	34
7.2	Verkkokaaviot	35
8	Hyökkäyspinnan minimointi	36
8.1	Verkon segmentointi	36
8.2	Palveluiden piilottaminen	37
9	Riskit	38
9.1	Tietovuodot	38
9.2	Järjestelmän ja tiedon integriteetti	38
9.3	Palvelunestohyökkäys	39
9.3.1	Peilaava sekä vahvistettu palvelunestohyökkäys	39
9.3.2	Volumetriset hyökkäykset	40
9.3.3	Palvelunestohyökkäykset organisaatiossa	40
10	Pohdinta	42
11	Yhteenveto	44
	Viitteet	45

Käytetyt symbolit ja lyhenteet

CISA	Cybersecurity and Infrastructure Security Agency
CPE	Common Platform Enumeration
CSP	Content Security Policy
CSRF	Cross-Site Request Forgery
CT	Certificate Transparency
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DNS	Domain Name System
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IoT	Internet of Things
LAN	Local Area Network
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
PaaS	Platform as a Service
RDP	Remote Desktop Protocol
SQL	Structured Query Language
SSH	Secure Shell Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
XSS	Cross-Site Scripting

1 Johdanto

Internetiin liitettävien laitteiden määrä kasvaa jatkuvasti, ja tietoverkkojen turvallisuuden ja tiedon eheyden varmistamisesta on tullut ensiarvoisen tärkeää. Samalla myös erilaisten ohjelmistojen määrä on kasvanut näissä laitteissa. Tähän kehitykseen liittyy kuitenkin ongelma: mitä enemmän laitteita liitetään internetiin, sitä haavoittuvammaksi organisaatio tulee. Hyökkäyspinnan kartoittaminen on eräs tapa mitata organisaation haavoittuvuutta internetistä tulevia uhkia kohtaan. Hyökkäyspinta tarkoittaa kaikkien niiden järjestelmän mahdollisten sisäänpääsypisteiden ja haavoittuvuuksien kokonaisuutta, joita hyökkääjä voi hyväksikäyttää vaarantaakseen järjestelmän turvallisuuden. Kun organisaatiot ja yksityishenkilöt jatkavat toimintojensa digitalisointia ja näin laajentavat verkkoläsnäoloaan, laajenee hyökkäyspinta vastaavasti, mikä luo lisää haasteita tietoturvaan vastaaville henkilöille.

Internetiin liitettävät laitteet ovat jatkuvasti erilaisten skannausten ja automatisoitujen hyökkäysten kohteena. Näitä laitteita skannaavat mm. hyökkääjät, verkkojen omistajat, tutkijat sekä valtiolliset toimijat. Esimerkiksi Palo Alto Networksin raportti kertoo, että haavoittuvan SSH-palvelimen murtaminen tapahtuu keskimäärin noin kolmessa tunnissa ¹. Usein haavoittuvuuksien hyväksikäyttöä edeltää järjestelmän skannailu. Hyökkääjät pyrkivät löytämään organisaation toiminnalle kriittisiä palveluita, kuten edellä mainittuja SSH-palveluita. Oman hyökkäyspinnan kartoituksella pyritään löytämään järjestelmien mahdolliset heikkoudet ennen kuin hyökkääjät löytävät ne. Tunnistamalla kriittiset palvelut hyökkäyspinnastaan on organisaation mahdollista suojata ne paremmin.

Työn tutkimuskysymykset ovat seuraavat:

- **Mitä tarkoittaa hyökkäyspinta?** Työn tavoitteena on luoda kattava käsitys hyökkäyspinnan käsitteestä ja sen merkityksestä tietoturvallisuuden kannalta.
- **Miten hyökkäyspintaa voi kartoittaa?** Työssä tutkitaan tekniikoita ja strategioita, joita uhkatoimijat sekä organisaatiot voivat käyttää hyökkäyspinnan haavoittuvuuksien löytämiseen.
- **Miten hyökkäyspinnan kartoittaminen auttaa tietoturvallisuuden edistämässä?** Työssä arvioidaan menetelmiä ja välineitä hyökkäyspinnan analysoimiseksi ja minimoimiseksi.

Koska aihe on laaja, keskitytään työssä hyökkäyspinnan kartoittamiseen tietoverkoissa.

Työn rakenne on seuraava. Luvussa 2 käydään läpi työn taustaa sekä motivaatiota hyökkäyspinnan kartoitukseen. Siinä määritellään myös hyökkäyspinta terminä sekä muita aiheeseen läheisesti liittyviä termejä. Luvussa 3 määritellään metriikkaa hyökkäyspintaan liittyen. Samassa luvussa käydään läpi myös aiempia tutkimuksia sekä käydään läpi, miksi olemassa olevat mittarit eivät ole välttämättä toimivia jokaiselle organisaatiolle. Työkaluja tietoverkkojen skannaamiseen käydään läpi luvussa 4. Luvussa käsitellään myös verkkotunnusten listausta sekä yleisimpiä portteja. Luvussa 5 vertaillaan yleisimpiä hakukoneita, joilla voi etsiä internetiin liitettyjä laitteita. Luvussa

¹<https://unit42.paloaltonetworks.com/exposed-services-public-clouds/>

6 keskitytään hyökkäyspinnan kartoittamiseen testiverkossa. Kartoituksessa käytetään työssä esiteltyjä työkaluja, joilla voi kartoittaa verkkoja kattavasti. Luvussa 7 ja 8 käydään läpi vastakeinoja hyökkäyspinnan kartoittamiseksi sekä keinoja hyökkäyspinnan minimoimiseksi. Luvussa 9 käydään läpi riskejä, joita liittyy huonosti suojattuihin palveluihin, jotka ovat avoimena internetiin. Lopuksi luvut 10 ja 11 päättävät tämän työn.

2 Tausta

Tässä luvussa kerrotaan taustaa työlle sekä kuvaillaan ongelmia tietoturvallisuuden mittaamisessa. Lopuksi luvussa määritellään työhön liittyviä termejä, jotta työn seuraaminen on helpompaa myös alaa tuntemattomille.

Organisaation tietoturvallisuuden mittaaminen on usein haastavaa, sillä tietoturva on laaja ala. Perinteisesti tietoturvan perustehtäväksi määritetään luottamuksellisuuden, eheyden ja saatavuuden turvaaminen [63]. Jokaista näistä ulottuvuuksista mitataan hieman eri tavalla, mikä vaikeuttaa kattavan ja yleistettävän mittauskehiksen luomista.

Lisäksi verkkouhat kehittyvät jatkuvasti ja hyökkäykset ovat yhä kehittyneempiä. Uusia hyökkäystapoja ja haavoittuvuuksia ilmaantuu säännöllisesti, joten ohjelmistoja on päivitettävä riittävän usein. Kuitenkaan pelkästään ohjelmistojen haavoittuvuuksien vakavuutta seuraamalla ei voida arvioida järjestelmän tietoturvaa. Lisäksi tuntemattomille, nollapäivähaavoittuvuuksille, ei ole aluksi vakavuusarviota, joten niiden vakavuutta ei voida arvioida samalla mittarilla kuin ennestään tunnettuja ohjelmistohaavoittuvuuksia.

Toisin kuin joillakin muilla aloilla, tietoturvasta puuttuvat tarkoin määritellyt ja yleisesti hyväksytyt mittarit. Absoluuttisia mittareita on vaikea kehittää, ja yksinkertaiset mittarit vaativat oletuksia. Nämä oletukset ovat mahdollisia haavoittuvuuksia. [64] Yleisesti hyväksytyjen standardimittareiden puuttuessa, organisaatioiden keskinäisen tietoturvan tasoa ei pysty vertailemaan helposti. Vaikka ISO 27001, NIST Cybersecurity -kehys ja muut vastaavat kehykset tarjoavat ohjeita, vaativat ne yleensä tietoturvaltaan kypsää organisaatiota. Lisäksi ne vaativat organisaatioilta resursseja ja asiaan perehtyneitä tietoturva-asiantuntijoita, sillä niihin kuuluu muun muassa tietoturvakontrollien tehokkuuden arviointi, haavoittuvuuksien tunnistaminen ja riskitasojen arviointi. Koska nämä arvioinnit ovat usein kuitenkin subjektiivisia, vaikuttaa niihin konteksti, kuten organisaation riskinottohalukkuus, toimialan määräykset ja teknologinen ympäristö, esimerkiksi pilviympäristössä on erilaisia riskejä kuin organisaation omiin konesaleihin perustuvissa ympäristöissä.

Turvallisuuden ja käytettävyyden tasapainottaminen on hankalaa ja tämän vuoksi tietoturvatoimenpiteet voivat joskus olla ristiriidassa käytettävyyden ja helppouden kanssa. Esimerkiksi vahvojen salasanakäytäntöjen käyttöönotto voi parantaa turvallisuutta, mutta vaikuttaa kielteisesti käyttäjäkokemukseen. Viime aikoina onkin nähty enemmän toteutuksia salasanattomille kirjautumisille tietotekniikka-alan suurilta yrityksiltä.²³⁴

Tietoturvallisuuden mittaamisen pitäisi olla jatkuvaa, sillä uudet haavoittuvuudet muuttavat organisaation tietoturvallisuutta. Eräs tapa arvioida järjestelmän tietoturvaa automaattisesti on kartoittaa sen hyökkäyspintaa. Tämä työ käsittelee pääosin MITREN ATT&CK -viitekehiksen mukaista tiedusteluvaihetta [41].

²<https://www.microsoft.com/en-us/security/business/solutions/passwordless-authentication>

³<https://blog.google/technology/safety-security/one-step-closer-to-a-passwordless-future/>

⁴<https://appleinsider.com/inside/ios-16/tips/how-to-use-passkeys-instead-of-passwords-on-ios-16>

2.1 Hyökkäyspinta

Hyökkäyspinnalla tarkoitetaan niiden järjestelmän rajapintojen joukkoa, joiden kautta mahdollinen hyökkääjä voi päästä järjestelmään sisään, löytää haavoittuvuuksia ja vahingoittaa sitä tai muuttaa sen toimintaa. Hyökkäyspinta voidaan siis nähdä mittarina järjestelmän haavoittuvuudelle. Haavoittuvammassa järjestelmässä on suurempi hyökkäyspinta, joten hyökkäyspinnan pienentäminen tekee järjestelmästä tietoturvallisemman [38].

Hyökkäyspinta voidaan jakaa kahteen osaan: digitaaliseen ja fyysiseen. Digitaalisella hyökkäyspinnalla tarkoitetaan organisaation tai yksittäisen henkilön digitaalisessa ympäristössä olevien kaikkien niiden potentiaalisten haavoittuvuuskohtien kokonaisuutta, joita verkkohyökkääjät voivat hyödyntää. Se siis käsittää kaikki digitaaliset resurssit, ohjelmistot, järjestelmät ja yhteydet, joista voidaan löytää haavoittuvuuksia. Esimerkiksi ohjelmistot, ohjelmointirajapinnat, portit ja palvelimet ovat digitaalista hyökkäyspintaa.

Fyysisellä hyökkäyspinnalla tarkoitetaan kaikkia organisaation tai järjestelmän fyysiseen infrastruktuuriin ja omaisuuteen liittyviä mahdollisia haavoittuvuuskohtia, joita hyökkääjät voivat hyödyntää. Toisin kuin digitaalinen hyökkäyspinta, jossa keskitytään ensisijaisesti digitaaliseen omaisuuteen ja kyberuhkiin, fyysinen hyökkäyspinta käsittelee konkreettisia, fyysisiä komponentteja [55]. Esimerkiksi rakennukset, toimistot, datakeskukset ja muut fyysiset sijainnit ovat osa fyysistä hyökkäyspintaa. Luvaton pääsy näihin paikkoihin voi johtaa tietomurtoihin, varkauksiin tai toiminnan keskeytymiseen. Tässä työssä kuitenkin keskitytään digitaaliseen hyökkäyspintaan.

Digitaalisen sekä fyysisen hyökkäyspinnan ymmärtäminen ja hallinta on ratkaisevan tärkeää kyberturvallisuuden kannalta, sillä suurempi hyökkäyspinta lisää kyberuhkien ja tietomurtojen uhkaa. Verkon hyökkäyspintaan vaikuttaa avoimet portit, niissä olevat avoimet palvelut ja niiden mahdolliset haavoittuvuudet sekä väärin konfiguroidut palvelut.

Verkon hyökkäyspinta voidaan määritellä myös sisään ja ulos tulevan datan kautta. [37][19] Tässä määrittelyssä jokainen rajapinta, jossa liikkuu dataa, on osa hyökkäyspintaa. Tätä tapaa voidaan käyttää erityisesti rajapintojen tutkimisessa ja uhkamallinnuksessa.

2.2 Terminologiaa

Haavoittuvuus on järjestelmän, sen mallin, toteutuksen tai sisäisen valvonnan heikkous, jota käyttämällä, joko tahallaan tai vahingossa, voidaan rikkoa järjestelmän tietoturvasääntöjä ja hyväksikäyttää järjestelmää. Haavoittuvuuksia on myös muualla kuin tietojärjestelmissä, esimerkiksi organisaation liiallinen riippuvuus tiettyyn energiamuotoon. [58] Tässä työssä kuitenkin keskitytään ohjelmistojen haavoittuvuuksiin.

Nollapäivähaavoittuvuus on haavoittuvuus, jolle ei ole vielä korjaustoimenpidettä ja jolle on jo hyväksikäyttömenetelmä. Nollapäivä viittaa siihen, että ohjelman kehittäjillä on nolla päivää aikaa korjata ongelma, kun haavoittuvuus julkaistaan tai sitä käyttävä haittaohjelma havaitaan.

Transmission Control Protocol (**TCP**) on yhteispohjainen eli tilallinen protokolla.

Sillä luodaan lähettäjän ja vastaanottajan välille yhteys, jota pidetään aktiivisena, kunnes kaikki tarvittavat paketit on lähetetty. TCP:ssä on mekanismeja, jotka mahdollistavat, että tieto vastaanotetaan ehjänä, vaikka yhteydessä olisikin ongelmia. Lähettäjä seuraa kaikkia lähetettyjä paketteja ajastimen avulla ja odottaa, että vastaanottajaa kuittaa ne. Jos kuittauspaketti ei saavu perille, lähettää alkuperäinen lähettäjä paketin uudelleen.

User Datagram Protocol (**UDP**) käyttää paljon yksinkertaisempaa tiedonsiirtomenetelmää kuin TCP. Siinä ei tarkisteta, onko vastaanottaja saanut paketit tai ovatko ne saapuneet oikeassa järjestyksessä. UDP on siis tilaton protokolla, sillä on eheysominaisuuksia vain tarkistussummien avulla. Se on siis yksinkertaisempi ja nopeampi tapa siirtää paketteja, minkä takia sitä käytetään yleensä palveluissa, joissa vaaditaan matalaa viivettä, esimerkiksi internet-puheluissa.

Hunajapurkki on systeemi tai palvelu, jonka tehtävänä on toimia houkuttimena hyökkäyksille. Sen tehtävänä on havaita hyökkääjiä, harhauttaa hyökkääjiä tai kerätä tietoa hyökkääjän käyttäytymisestä järjestelmässä. Hunajapurkkeja voidaan käyttää myös uusien hyökkäysten tai haavoittuvuuksien tunnistamisessa. Hunajapurkeilla voidaan myös tutkia, mitä portteja hyökkääjät kartoittavat skanneillaan. [62]

3 Haavoittuvuusmetriikat

Tässä luvussa kerrotaan erilaisia mittareita tietoturvallisuuden ja hyökkäyspinnan kartoittamiseen. Luvussa käydään myös läpi aiempia tutkimuksia. Tietoturvallisuuden mittaaminen on vaikeaa ja usein hidasta, joten tutkimuksissa on ehdotettu erilaisia tapoja mitata sitä.

3.1 CVSS haavoittuvuuksien pisteytykseen

Common Vulnerability Scoring System (CVSS) on standardoitu viitekehys ohjelmistojen haavoittuvuuksien vakavuuden arvioimiseksi ja luokittelemiseksi [15]. Sen avulla on mahdollista mitata ohjelmistojen tietoturva-aukkojen vaikutusta kvantitatiivisesti ja kvalitatiivisesti, mikä helpottaa organisaatioiden haavoittuvuuksien korjaamisen priorisointia. Tässä viitekehyksessä annetaan jokaiselle haavoittuvuudelle pistearvo.

CVSS-pisteet ovat standardoitu tapa kvantifioida ja mitata ohjelmistojen haavoittuvuuksien vakavuutta. Ne esitetään numeroarvoina, ja korkeampi numeroarvo tarkoittaa vakavampaa haavaa. CVSS:n perusmittariryhmä kuvaa haavoittuvuuden ominaispiirteitä, jotka pysyvät muuttumattomina eri aikoina ja eri käyttöympäristöissä. CVSS kategorisoi haavoittuvuudet pisteiden mukaan neljään kategoriaan: matala, keskitaso, korkea ja kriittinen. Vakavimmat haavoittuvuudet ovat kriittisiä [48], kuten Microsoft Exchangeen kesällä 2023 (CVE-2023-21709) julkaistu käyttöoikeuksien korotuksille altistava haavoittuvuus. CVSS ei ole varsinainen mittari järjestelmän tietoturvallisuudelle, se kertoo vain havaitun haavoittuvuuden vakavuuden. Se on myös huono mittari laitteen tietoturvallisuudelle, koska se ei huomioi, kuinka paljon laitteen tietoturvaa on tutkittu. Esimerkiksi Siemensin Simatic S7:ssä, jota on tutkittu Stuxnetin takia paljon, on enemmän julkaistuja haavoittuvuuksia kuin muissa ohjelmoitavissa logiikoissa.

CVSS-pisteet eivät sovellu tietoturvallisuuden mittaamiseen, sillä osa haavoittuvuuksista on ns. nollapäivähaavoja, joilla ei välttämättä ole määriteltä pistearvoa [67]. Haavoittuvuuden julkaisusta saattaa kulua useita päiviä ennen kuin se on analysoitu ja sille on annettu pistearvo [13]. Ei siis ole mahdollista luottaa pelkästään CVSS-arvoon, sillä uusissa haavoittuvuuksissa joudutaan tekemään omaa arviointia haavoittuvuuksien kuvauksista.

3.1.1 CVSS-hyökkäysvektorit

CVSS määrittää haavoittuvuuksille hyökkäysvektorit, jotka kertovat miten haavoittuvuutta on mahdollista hyväksikäyttää. Nämä hyökkäysvektorit vaikuttavat myös haavoittuvuuden pistearvoon. Tyypillisesti verkon yli hyväksikäytettävät haavoittuvuudet saavat suuremmat pistearvot kuin muiden hyökkäysvektorien haavoittuvuudet. CVSS:ssä on neljä hyökkäysvektoria: verkko (network, N), lähekkäin (adjacent, A), paikallinen (local, L) ja fyysinen (physical, P). [14]

- **Verkko (network)** Haavoittuvuutta voidaan hyödyntää etänä ilman, että kohdeeksi joutuneeseen järjestelmään on pääsy. Tämä tarkoittaa, että hyökkääjä voi hyödyntää haavoittuvuutta verkkoyhteyden, kuten internetin, kautta. Tällaista haavoittuvuutta kutsutaan usein etähyödynnettäväksi.

- **Lähiverkko (adjacent, A)** Haavoittuvuutta voi hyödyntää hyökkääjä, jolla on pääsy lähiverkkoon, jossa kohteena oleva järjestelmä on. Lähekkäin oleva haavoittuvuus on verkkopinossa, eikä hyökkäystä voi siten tehdä toisesta loogisesta verkosta käyttämällä esimerkiksi reititintä. Esimerkiksi hyökkääjä, joka on samassa lähiverkossa kuin kohdejärjestelmä, voi hyödyntää haavoittuvuutta.
- **Paikallinen (local, L)** Haavoittuva komponentti ei ole hyväksikäytettävissä verkon yli, vaan hyökkääjän pitää pystyä kirjautumaan laitteelle. Haavoittuva komponentti ei ole sidottu verkkopinoon, vaan hyökkääjän reitti kulkee luku-, kirjoitus- tai suoritusominaisuuksien kautta. Hyökkäykseen siis vaaditaan järjestelmään sopivat oikeudet, jotka hyökkääjä voi saada hyödyntämällä toista haavoittuvuutta tai hankkimalla tunnukset kirjautumiseen oikealta käyttäjältä.
- **Fyysinen (physical, P)** Haavoittuvuutta voi hyödyntää vain käyttäjä, jolla on suora fyysinen pääsy haavoittuvaan komponenttiin. Esimerkiksi, CVE-2022-45888 vaatii USB-laitteen fyysisen irrottamisen, jotta haavoittuvuutta voi hyväksikäyttää.

3.1.2 CPE järjestelmien yksilöintiin

Common Platform Enumeration (CPE) on National Institute of Standards and Technology (NIST) ylläpitämä nimeämisstandardi laitteistojen, käyttöjärjestelmien ja ohjelmistojen tunnistamiseksi. CPE:n avulla voidaan järjestelmän osista tunnistaa niiden versiot ja päivitykset. [47] Järjestelmien ylläpitäjät voivat käyttää CPE-arvoja pitääkseen kirjaa järjestelmän osista. Koska CPE-arvot ovat uniikkeja, on niiden avulla mahdollista automatisoida päivityspäätöksiä. Ihanteellisessa tapauksessa järjestelmän kaikille osille on määritetty CPE-arvo, jolloin uusista haavoittuvuuksista tulee automaattinen ilmoitus.

Avoimesti versiotietonsa kertova palvelu on haavoittuvammassa asemassa kuin palvelu, joka ei paljasta itsestään tietoja [8]. Jos tiedetään avoimen palvelun versiotiedot (CPE), voidaan sille hakea haavoittuvuudet helposti internetistä löytyvistä avoimista tietokannoista. Pahimmassa tapauksessa versiotietojen avulla hyökkääjä voi ajaa automaattisia hyökkäyksiä haavoittuvuuksien perusteella. Tässä tapauksessa hyökkääjän ainoaksi tehtäväksi jää porttiskannaus, joka on usein myös automatisoitua. CPE-arvojen kartoittamiseen voidaan käyttää Nmapia, josta kerrotaan lisää Luvussa 4.2.1. Hyökkääjä voi myös käyttää internetin hakukoneita etsiäkseen haavoittuvia palveluita CPE-arvon avulla. Luvussa 5 on kerrottu lisää hakukoneista.

Esimerkiksi CPE-arvo Red Hat Enterprise Linux versio 9.0:lle on

```
cpe:2.3:o:redhat:enterprise_linux:9.0:*:*:*:*:*:*
```

Tässä "o" tarkoittaa käyttöjärjestelmää, "redhat" on järjestelmän toimittajan nimi ja "enterprise_linux" on tuotteen nimi. Tässä tapauksessa järjestelmän versio on 9.0. Versionumeron jälkeiset lisäversion tarkenteet (asteriskit) eivät ole pakollisia. Kyseiselle järjestelmälle löydetään NIST:n CPE-tietokannasta yli kaksisataa haavoittuvuutta [49].

3.2 Hyökättävyys

Aiemmat tutkimukset ovat arvioineet järjestelmän tietoturvaa hyökättävyyssmittarilla. Tutkimuksissa on todettu, että absoluuttisen tietoturvan mittaaminen ei ole mielekäästä. Usein on kannattavampaa mitata suhteellista tietoturvaa eli vertailla samankaltaisia järjestelmiä toisiinsa. Tutkimuksen kehittämä hyökättävyyssmittari huomioi mahdollisten ohjelmointivirheiden eli bugien hyväksikäytön helppoutta ja seurauksia. Tutkimuksen mukaan järjestelmissä on olemassa tiettyjä ominaisuuksia, jotka ovat todennäköisemmin mahdollisia hyökkäyskohteita kuin toiset. Näiden järjestelmäominaisuuksien määrä määrittää järjestelmän hyökättävyyden. [22]

Tätä hyökättävyyssmittaria ei ole kuitenkaan mielekäästä käyttää kahteen erilaiseen järjestelmään, koska niissä on erilaiset hyökkäysvektorit, eikä saatuja tuloksia voida vertailla. Lisäksi hyökättävyyssmittari vaatii laajaa järjestelmän tuntemista ja tietoturvasiantuntijoita analysoimaan järjestelmään, joten hyökättävyyssmittarin käyttäminen vaatii tietoturvaltaan kypsää organisaatiota.

4 Hyökkäyspinnan kartoitus

Tässä luvussa käsitellään erilaisia tapoja kartoittaa järjestelmien hyökkäyspintaa. Aluksi käydään läpi porttiskannauksen taustaa kertomalla eri porttityypeistä. Sen jälkeen tekstissä kuvataan erityyppisiä skannauksia ja niiden eroja. Luvussa käydään myös läpi työkaluja skannaamiseen. Lopuksi käydään vielä läpi verkkotunnusten listaamista.

4.1 Porttiskannaus

Jokaisessa verkon laitteessa on 65535 porttia. Internet Assigned Numbers Authorityn (IANA) ylläpitämässä rekisterissä on määritetty porteille eri käyttötarkoituksia. Portit 1-1023 ovat IANA:n määrittelemiä systeemiportteja (system ports tai well known ports). Niiden käyttäminen Unix-pohjaisissa käyttöjärjestelmissä vaatii prosessilta pääkäyttäjän oikeudet, jotta systeemiportteihin yhdistävät asiakkaat voivat luottaa siihen, että portissa toimiva palvelu on pääkäyttäjän hyväksymä eikä koneen muun käyttäjän pyörittämä väärä palvelu [10]. Tämä on tärkeää esimerkiksi yliopiston kaltaisessa ympäristössä, jossa useilla käyttäjillä voi olla laaja pääsy järjestelmään. Nykyään suosittelumpi tapa varmistua palvelun oikeellisuudesta on käyttää varmenteita.

Käyttäjäportit tai rekisteröidyt portit on numeroitu välille 1024-49151. IANA:n ylläpitämässä rekisterissä on siis määritetty kaikki portit välillä 0-49151 [23]. Loput porteista (49152-65535) ovat tyypiltään dynaamisia, eikä niitä voi rekisteröidä IANA:lle. [7]

Yksi tapa kartoittaa hyökkäyspintaa on ajaa porttiskanneja. Porttiskannissa kartoitetaan avoimia portteja järjestelmässä. Jos portti on avoin, tulkitaan siinä olevan avoin palvelu. Jokainen avoin palvelu lisää hyökkäyspintaa ja on potentiaalinen tietoturva-uhka. Porttiskannaus on usein myös hyökkääjien ensimmäinen askel järjestelmään pääsyyn. Ilman lupaa tehty porttiskannaus voidaan nähdä tietomurron yrityksenä.

Porttiskannausta käytetään yleisesti tunkeutumistestauksessa ja tietoturva-auditoinneissa. Yleensä kohteen kaikki portit skannataan [27]. Porttiskannauksissa löytyy usein yllättäviäkin havaintoja, koska ohjelmistot saattavat avata portteja ilman, että kehittäjät ja ylläpitäjät tietävät niistä. Erityisesti esineiden internetin (Internet of Things, IoT) -laitteissa voi olla erikoisiakin portteja auki.

Porttiskannauksen tulokset voivat olla erilaisia riippuen, mistä skannia ajetaan. Sisäverkossa skannaustyökalu näkee ja tunnistaa enemmän palveluita kuin ulkopuolisesta verkosta ajettu skanni. Tulokset tosin riippuvat palomuurin asetuksista sekä esimerkiksi internetpalveluntarjoajan pakettisuodatuksista.

Laajoissa skannauksissa on usein järkevämpää jakaa skannit kahteen tai useampaan osaan. Ensimmäisellä skannauksella pyritään löytämään mahdollisimman paljon avoimia portteja sekä kaikki internet-protokollan (IP) osoitteet, joissa on palveluita. [44] Ensimmäisiä skannauksia ajetaan yleensä työkalulla, joka pystyy suorittamaan skannauksia nopeasti, esimerkiksi ZMap tai masscan. Toisessa skannauksessa tarkennetaan ensimmäisen skannin havaintoja ja yleensä pyritään tunnistamaan palveluiden versioita sekä mahdollisia haavoittuvuuksia. Näitä skanneja voidaan ajaa ensimmäisen

skannissa löydettyihin portteihin tai käyttää valmiita listoja suosituimmista palveluista ja porteista. Suosituimmista porteista kerrotaan lisää luvussa 4.5.

4.1.1 Aktiivinen skannaus

Aktiivisessa skannauksessa kohteeseen lähetetään koetinpaketteja samalla kuunnellen vastauksia niihin. Koetinpaketit voivat olla generisiä, kuten TCP-yhteyden kättely, tai sovelluskohtaisia. Aktiivisissa skanneissa järjestelmälle luodaan sormenjälki, josta tietoja parsimalla voidaan päätellä ohjelmiston versiotunnisteet, kuten CPE-arvo. [4]

```
SF-Port53-TCP:V=7.93%I=7%D=4/10%Time=6434618C%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x82\0\x01\0\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
```

Kuva 1: Nmapin luoma sormenjälki eräästä palvelusta.

Nmap pyrkii tunnistamaan järjestelmän versioita muodostamalla yhteyden avoimeen TCP-porttiin ja tulostamalla kaiken datan, mitä portissa kuunteleva palvelu lähettää takaisin. Esimerkiksi Nmap tunnistaa käyttöjärjestelmiä niiden vastauksista yhteydenottopyyntöihin. Se voi tunnistaa käyttöjärjestelmät niiden eri muotoisten aikaleimojen perusteella. Kuvassa 1 on esimerkki eräästä Nmapin luomasta sormenjäljestä, josta voi päätellä kohteen olevan Linux-pohjainen järjestelmä.

Aktiivisella skannauksella ei välttämättä tunnisteta verkossa olevia tietokoneita, joiden palvelut ovat avoinna vain hetken. Aktiivinen skannaus voi olla myös melko häiritsevää skannattavalle laitteelle, joten sitä ei välttämättä voi käyttää teollisuusautomaatiolaitteiden skannaamiseen [56]. Teollisuusautomaatiolaitteet ovat usein rajatumpia prosessoriteholtaan kuin tyypilliset verkkopalvelimet. Lisäksi ne ovat usein yritykselle kriittisiä, eikä niiden saatavuushäiriöitä sallita. Tämän takia laitteita ei tulisi skannata kuin huoltokatkojen aikana [33].

4.1.2 Passiivinen skannaus

Passiivisessa skannauksessa ei lähetetä kohteeseen mitään tietoa, vaan siinä tarkkaillaan palvelimien liikennettä erillisestä havaintopisteestä tietoverkossa. Havaintopisteeseen voidaan asentaa laite tai ohjelmisto, joka mahdollistaa passiivisen tarkkailun. Koska passiivisessa skannauksessa ei lähetä kohteeseen paketteja, on sen havaitseminen vaikeampaa kuin aktiivisen skannauksen. Se ei myöskään kuluta kohteen verkkokapasiteettia yhtä paljon. Passiivisessa skannauksessa on kuitenkin oltava samassa lähiverkossa kohteen tai sen palomuurin kanssa. Tällainen skannaus on jatkuvaa, joten sillä on mahdollista havaita laitteita, joiden portti on vain hetken auki. Wireshark on tunnetuimpia passiivisia tarkkailuohjelmistoja [56].

4.1.3 Häiritsevä skannaus

Häiritsevällä skannauksella tarkoitetaan kartoitusta, joka joko kuluttaa kohdejärjestelmän resursseja paljon tai hyväksikäyttää olemassa olevaa haavoittuvuutta. Häiritseviksi

skannauksiksi lasketaan myös skannaukset, jotka muuttavat skannattavan kohteen tilaa. Häiritsevä skannaus on tarkempi kuin passiivinen skannaus, koska sillä voidaan varmentaa havaittu haavoittuvuus.

Esimerkiksi Nmap kategorisoi häiritseväksi skriptin, joka kokeilee tyhjää salasanaa mysql-palvelun pääkäyttäjälle [24]. Häiritsevä skannaus voi aiheuttaa kohdejärjestelmälle palvelunestotilan, joten sen käyttäminen vaatii huolellisuutta.

4.2 Työkaluja skannaamiseen

Tässä luvussa esitellään työkaluja verkkojen skannaamiseen. Verkon skannaustyökalut ovat välttämättömiä hyökkäyspinnan tunnistamisessa. Suurten verkkojen skannaamiseen on usein käytettävä nopeita työkaluja, kuten masscania tai ZMapia. Nopeiden skannausten tuloksia voidaan vielä tarkentaa erillisillä sovelluskohtaisilla skannauksilla. Pienten verkkojen skannaamiseen riittää hitaampikin työkalu. Usein hitaammat työkalut tuottavat hieman tarkemman tuloksen.

4.2.1 Nmap

Nmap on avoimen lähdekoodin tietoverkkojen kartoitusohjelmisto. Sitä voidaan käyttää myös tietoverkon tietoturvallisuuden testaamiseen. Nmapin avulla verkosta voidaan etsiä avoimia palveluita ja tunnistaa niiden ohjelmisto-, käyttöjärjestelmä- ja laitteistoversioita. Yksi ensimmäisistä vaiheista missä tahansa verkkoskannauksessa on vähentää IP-osoitteiden joukko aktiivisten tai kiinnostavien tietokoneiden listaksi. Jokaisen IP-osoitteen jokaisen portin skannaaminen on hidasta ja yleensä tarpeetonta. Kiinnostavien tietokoneiden määrittely riippuu tietenkin skannauksen tarkoituksesta. Verkon ylläpitäjät saattavat olla kiinnostuneita vain laitteiden palveluista, jotka ovat tietyssä portissa, kun taas tietoturvatestaajat ovat yleensä kiinnostuneita jokaisesta laitteesta ja avoimesta portista. Tietoturvatestaajat saattavat käyttää näiden laitteiden kartoittamiseen esimerkiksi Nmapin *ping skannia*. Siinä kartoitetaan, mitkä osoitteet vastaavat ylipäätään mitään. Ping skannissa käytetään yleensä muitakin tekniikoita kuin tavallisia Internet Control Message Protokollaan kuuluvia ICMP-echo-pyyntöjä, koska usein ne on estetty palomureissa. [50]

Version tunnistuksessa Nmap yrittää päätellä palvelimen ohjelmistoja ja niiden versioita. Version tunnistuksessa Nmap lähettää sopivan muotoisia paketteja kohdeporttiin ja pyrkii päättelemään niiden vastauksista palvelun ja sen version. Nmap pyrkii myös saamaan palvelulle CPE-arvon, jonka avulla palvelulle voidaan hakea haavoittuvuuksia tietokannoista. [53]

```
22/tcp open  ssh  OpenSSH 7.9p1 Raspbian 10+deb10u2+rpt1 (protocol 2.0)
|_ banner: SSH-2.0-OpenSSH_7.9p1 Raspbian 10+deb10u2+rpt1
```

Kuva 2: Nmapin tekstinkaappausskriptin tulos Raspberry PI -laitteesta.

Nmapilla skannatessa käytetään usein myös tekstinkaappausskriptiä, joka yrittää avata TCP-yhteyden haluttuun porttiin ja kuuntelee muutaman sekunnin tekstivas-

tauksia. Kuvassa 2 on esitetty Nmapin tekstinkaappausskriptin tulos Raspberry PI -laitteessa. Vastauksesta nähdään, että kyseinen laite on todennäköisesti Raspberry ja kyseisessä portissa on SSH-palvelu. Tähän SSH-palveluun voitaisiin suorittaa myös Nmapin skripti, joka kokeilee eri salasanoja ja pyrkii etsimään niin oikean salasanan sisäänkäyntiin.

Perusasetuksilla Nmap skannaa tuhat yleisintä porttia [51]. Suurten verkkojen kaikkien porttien skannaamiseen ei yleensä kannata käyttää Nmapia, koska Nmap on synkroninen eli se odottaa vastausta lähettämäänsä pyyntöön, eikä se siis pysty lähettämään samasta säikeestä samaan aikaan uusia pyyntöjä, mikä tekee siitä verrattain hitaan. Asynkroniset skannaustyökalut taas lähettävät useita pyyntöjä rinnakkain eivätkä jää kuuntelemaan vastausta samassa säikeessä.

4.2.2 Masscan

Masscan on avoimen lähdekoodin verkkoskannaustyökalu, joka on suunniteltu erityisesti suurten verkkojen skannaamiseen. Se käyttää omaa verkkopinoa, mikä mahdollistaa suurten verkkojen nopean skannaamisen. Se lähettää TCP-SYN -paketteja asynkronisesti, eli se lähettää pyynnön eikä jää odottamaan vastausta siihen, vaan siirtyy lähettämään seuraavan pyynnön. Masscan pystyy siihen käyttämällä vain kahta säiettä: yksi on pakettien lähettämiseen ja toinen niiden vastaanottamiseen, eikä vastauksen odottaminen siis estä lähetyssäiettä. Se ei pidä muistissa mitään tilaa, eikä se siis muista lähettämiään paketteja. Masscanin lähetys- ja vastaanottosäikeet toimivat itsenäisesti ilman synkronointia. [21]

Masscan soveltuukin asynkronisuutensa takia suurten verkkojen sekä porttimäärien skannaamiseen. Koska masscan satunnaistaa kohdelistan, ei sen pitäisi kuormittaa yksittäistä verkkoa liikaa. Luvun 6 skannauksessa on käytetty aluksi masscania.

4.2.3 ZMap

ZMap on toinen tapa, masscanin lisäksi, ajaa asynkronisia skanneja isoihin verkkoihin. ZMap on suunniteltu koko internetin skannaamiseen, sillä voi skannata koko internetin alle tunnissa [12]. Uudemmissa päivityksissä työkalu tekee saman alle viidessä minuutissa [69]. Koska ZMap lähettää vain yhden paketin IP-osoitteeseen eikä jää odottamaan vastauksia, on se yli 1300 kertaa nopeampi kuin Nmap aggressiivisimmilla asetuksilla. ZMap voi skannata 1,37 miljoonaa pakettia per sekunti. [12]

Koska lähetysnopeus on niin korkea, on hyvä huomioida eri verkkojen erilaiset kapasiteetit ja koordinoita skanneja verkon ylläpitäjien kanssa sekä arvioida sopiva maksimilähetysnopeus. ZMapista saatua dataa voidaan käyttää tarkempien skannausten suorittamisessa. Niihin voidaan käyttää muun muassa ZGrabia.

4.2.4 ZGrab

ZGrab on avoimen lähdekoodin verkkoskannaustyökalu, joka on suunniteltu skannaamaan sovelluserroksen protokollia. Sen on luonut ZMap-projektiryhmä ja se on luotu toimimaan ZMapin kanssa. ZMap tunnistaa skanniin vastaavat laitteet, ja ZGrab

```

{
  "status": "success",
  "protocol": "ssh",
  "result": {
    "server_id": {
      "raw": "SSH-2.0-OpenSSH_7.9p1 Raspbian-10+deb10u2+rpt1",
      "version": "2.0",
      "software": "OpenSSH_7.9p1",
      "comment": "Raspbian-10+deb10u2+rpt1"
    }
  },
  "timestamp": "2023-04-10T20:16:50Z"
}

```

Kuva 3: Ote ZGrab:n palauttamasta datasta.

tunnistaa sovelluskerroksen protokollan niiden avoimista palveluista. ZGrab kerää avoimissa porteissa toimivien palvelujen tai sovellusten kertomia otsikko- ja metatietoja. Palveluiden vastauksia analysoimalla ZGrab antaa tietoa kyseisten palveluiden asetuksista, versioista ja mahdollisista haavoittuvuuksista. [68] [11]

Kuvassa 3 on ote ZGrab:n SSH-skannauksen tiedoista. ZGrab on tunnistanut oikein palvelimelta SSH-palvelun ja sen version.

4.3 UDP-porttien skannaus

UDP-porttien skannaaminen on hankalampaa ja usein hitaampaa. UDP on yhteydetön ja tilaton protokolla, eli skannauslaitteen ja kohdejärjestelmän välillä ei ole kättelyprosessia. Skannauslaite ei siis saa samanlaista kuittausta yhteydestä kuin TCP:ssä.

Kun UDP-paketti lähetetään suljettuun porttiin, kohdejärjestelmä voi vastata ICMP-viestillä *Port Unreachable* eli portti on saavuttamattomissa. Kaikki järjestelmät eivät kuitenkaan lähetä tätä vastausta, jolloin on vaikea erottaa toisistaan suljettuja portteja ja portteja, jotka ovat pudottaneet äänettömästi paketin.

Nmap skannaa UDP-portteja lähettämällä ensin niihin protokollakohtaisen paketin. Yleensä vain oikeat palvelut vastaavat pakettiin ja ne merkitään avoimiksi. Muut palvelut vain pudottavat paketin äänettömästi eivätkä siis vastaa mitään. Muihin kuin tunnettuihin ja yleisimpiin portteihin Nmap lähettää tyhjän UDP-paketin. Yleensä palvelu pudottaa tyhjän paketin lähettämättä vastausta. Jos Nmap ei saa vastausta lähettämäänsä pakettiin, odottaa se käyttäjän määrittelemän ajan aikakatkaisua. Koska jotkut UDP-palvelut vastaavat paketteihin hitaasti, joutuu Nmapin käyttäjä yleensä määrittelemään melko pitkän aikakatkaisun, jotta Nmap tunnistaisi palvelut oikein.

Yleensä palomuurit on konfiguroitu niin, että verkon ulkopuolelta tulevat paketit pudotetaan vastaamatta mitään. Lisäksi palomuurit usein suodattavat UDP-liikennettä. Eli, jos vastausta lähetettyyn pakettiin ei tule, ei voida suoraan päätellä porttien tiloista mitään. Myös osoitteiden kääntäminen saattaa aiheuttaa ongelmia. [27] [52]

Toisaalta UDP:tä voidaan käyttää helpommin palvelunestohyökkäyksiin, koska siinä lähettäjän osoitteen väärentäminen on helpompaa. Lisäksi joillain UDP-protokollilla voidaan saada jopa 200-kertainen vahvistus hyökkäykselle. Palvelunestohyökkäyksistä kerrotaan lisää luvussa 9.3.

4.4 IPv6-osoitteiden skannaus

Internet Protocol versio kuudessa (IPv6) verkot ovat huomattavasti suurempia kuin aiemman Internet Protocol versio neljän (IPv4) verkot, joten skannaaminen tehdään yleensä eri tavalla. Yksinkertainen kaikkien osoitteiden skannaaminen ei ole mahdollista IPv6-verkossa. IPv6:ssa osoitteita jaetaan yleensä 64-bitin aliverkkoina [5]. 64-bitin aliverkko on siis 2^{32} kertaa suurempi kuin koko IPv4-osoiteavaruus. Koska IPv6-osoiteavaruus ja aliverkot ovat huomattavasti laajempia kuin koko IPv4-osoiteavaruus, eroavat skannausmenetelmät merkittävästi toisistaan.

IPv6-verkkojen skannaus perustuu usein valmiiksi kerättyihin IP-osoitelistoihin. Niitä kerätään, esimerkiksi läpikäymällä joko DNS:ää tai avoimia varmennelekeja. [17] Kartoitettavien verkkojen määrää voi myös pienentää arvaamalla osia verkko-osoitteista. Automaattinen IP-osoitteiden jakaminen saattaa jakaa vierekkäisiä osoitteita, jolloin läpikäytävien osoitteiden määrä putoaa 64 bitistä kahdeksasta kuuteentoista bittiin. Osoitteissa saatetaan myös asettaa vain vähiten merkitsevät tavut, jolloin osoitteiden määrä putoaa 16 bittiin. Lisäksi virtualisointijärjestelmien osoitteet ovat usein arvattavissa. [20]

4.5 Yleisimmin skannatut portit

Tässä luvussa kerrotaan palveluista, joiden ei tulisi näkyä internetiin sekä porteista, joita käytetään yleisesti hyökkäyksissä. Hyökkäyspinnan kannalta tietyissä palveluissa on huomattavasti suurempi riski kuin toisissa. Niiden haavoittuvuuksien hyväksikäytön seuraukset ovat vakavampia tai ne ovat muuten yleisesti hyökkääjien kohteena. Yleensä hyökkääjien kohteiksi valikoituu kuitenkin mahdollisimman suurivaikutteisia palveluita. Tällaisia palveluita ovat esimerkiksi SSH-, VPN- sekä RDP-palvelut, jotka mahdollistavat etäkäytön tai pääsyn organisaation sisäverkkoon.

Myös portti 3306 on yleisimpien porttien listalla. Se on yleisesti käytetty MySQL-tietokantaportti. Hyökkääjät ovat kiinnostuneita organisaatioiden datasta, jolla voi joko kiristää organisaatiota tai jolla voi olla muuta rahallista arvoa. Hyökkääjät kartoittavat tietokantaportteja, koska löytämällä tietokantapalvelun ja mahdollisen haavoittuvuuden siitä, voivat hyökkääjät saada organisaation datan itselleen.

Yleisimpien skannattujen porttien listalla on myös portteja, joissa yleensä olevia palveluita voi käyttää palvelunestohyökkäyksiin. Portti 53 on tällainen portti. Siinä on yleensä DNS-palvelu, jota voi mahdollisesti käyttää palvelunestohyökkäyksiin. Palvelunestohyökkäyksistä kerrotaan enemmän luvussa 9.3.

Joskus palveluiden ylläpitäjät avaavat palvelulle jonkin toisen kuin yleisesti tunnetun portin. Tämä voidaan tehdä turvallisuussyistä, ristiriidoista muiden palvelujen kanssa tai muista erityisvaatimuksista. Jos esimerkiksi HTTPS:n vakioportti 443 on jo jonkin toisen sovelluksen käytössä, voidaan verkkopalvelinohjelmisto määrittää

kuuntelemaan vaihtoehtoista porttia, kuten 8443, sen sijaan. Vastaavasti, jos ylläpitäjä haluaa lisätä ylimääräisen turvallisuuskerroksen, voi hän asettaa SSH:n käyttämään standardista poikkeavaa porttia oletusportin 22 sijasta. Täytyy kuitenkin muistaa, että palvelun tietoturva ei voi perustua pelkästään siihen, ettei palvelua löydetä.

Nmapissa on nmap-services-tiedosto, joka on listaus porttien nimistä ja niitä vastaavista numeroista sekä protokollista. Jokaisella rivillä on luku, joka kuvaa sitä, kuinka todennäköisesti kyseinen portti on auki. [54]

Taulukossa 1 on valikoituna kymmenen yleisintä TCP-palvelua, porttia sekä niiden esiintyvyys nmap-services-tiedostosta. Ensimmäisessä sarakkeessa on palvelun nimi tai lyhenne, joka näkyy Nmapin tulosten service-sarakkeessa. Toisessa sarakkeessa on portin numero ja protokolla, jotka on erotettu toisistaan vinoviivalla. Kolmannessa sarakkeessa on esiintyvyys, joka kertoo, kuinka usein kyseinen portti oli auki Nmap-organisaation internetin tutkimuksissa. On huomattava, että Nmap ei listaa vaihtoehtoisia portteja, joten tulokset saattavat erota muiden organisaatioiden keräämistä hunajapurkkidatoista.

Taulukko 1: Nmap-organisaation määrittämät suosituimmat TCP-portit.

Palvelun nimi	Portti ja protokolla	Esiintyvyys
http	80/tcp	48,4%
telnet	23/tcp	22,1%
https	443/tcp	20,9%
ftp	21/tcp	19,8%
ssh	22/tcp	18,2%
smtp	25/tcp	13,1%
ms-wbt-server	3389/tcp	8,4%
pop3	110/tcp	7,7%
microsoft-ds	445/tcp	5,7%
netbios-ssn	139/tcp	5,1%

Suosituimmista porteista on suurempi riski, koska perusasetuksilla Nmap skannaa yleisimmät portit, joten hyökkääjä myös skannaa ne todennäköisimmin. SANS-instituutin Internet Storm Center -hunajapurkkidata listaa yleisimmiksi porteiksi myös vaihtoehtoisia portteja. SANSin datassa onkin useampi vaihtoehtoinen portti Hypertext Transfer Protocol (HTTP)-pohjaisille palveluille, kuten portti 8000 tai 8080 [60].

4.6 Verkkotunnusten listaus ja luettelointi

Nimipalvelujärjestelmä (Domain Name System, DNS) on hajautettu järjestelmä, joka muuntaa ihmisten luettavissa olevat verkkotunnukset numeerisiksi IP-osoitteiksi, joiden avulla tietokoneet tunnistavat toisensa verkossa. DNS-luettelointi on prosessi, jossa kerätään verkkotunnustietoja organisaation verkkoinfrastruktuurin kartoittamiseksi. Siinä voidaan käyttää nimipalvelujärjestelmää tietolähteenä, jonka avulla kohteesta

DNS Name: aalto.fi
DNS Name: 5g-research.aalto.fi
DNS Name: abe.aalto.fi
DNS Name: accounting.aalto.fi

Kuva 4: Aalto-yliopiston verkkotunnuksia.

voidaan kerätä esimerkiksi laitteiden ja palveluiden nimiä, käyttöjärjestelmäversioita, käyttäjätunnuksia, IP-osoitteita sekä aliverkkotunnuksia. DNS-luetteloinnin päätaavoitteena on kerätä mahdollisimman paljon tietoa kohdejärjestelmästä mahdollisten haavoittuvuuksien tunnistamiseksi.

Transport Layer Security (TLS) on salausprotokolla, jolla voidaan salata yhteys tietokoneiden välillä. TLS-salaus perustuu varmenteisiin eli sertifiikaatteihin, joilla viestinnän toinen osapuoli voi varmistaa, että kommunikoidaan oikean tahon kanssa. Näistä varmenteista on mahdollista kerätä verkkotunnusten listaa. Esimerkiksi aalto.fi-sivun varmenteesta nähdään, että muun muassa kuvan 4 mukaiset verkkotunnukset ovat käytössä samalla varmenteella.

Sisällön turvallisuuspolitiikka (content security policy, CSP) kertoo, mitkä ovat sallittuja resursseja ja niiden lähteitä kyseisellä sivustolla. CSP välitetään HTTP-vastauksen otsaketiedoissa ja sitä käytetään torjumaan muun muassa sivustojen välisiä hyökkäyksiä sekä injektiohyökkäyksiä [43]. CSP-otsakkeista voi kuitenkin hakea verkkotunnustietoja.

Kuvassa 5 on esitetty Aalto-yliopiston sivuilta löydetyt CSP-otsakkeet. Child-src *: sallii upotetun sisällön hakemisen mistä tahansa URL-osoitteesta. Connect-src sallii yhteyksien luonnin vain kyseiseen URL-osoitteeseen sekä mainittuun Amazon Web Services -URLiin.

```
default-src 'self';  
child-src *;  
style-src 'self';  
script-src 'self';  
img-src 'self' data: ;  
connect-src 'self' https://sis-aalto-prod-tasku.s3.eu-north-1.amazonaws.com
```

Kuva 5: Aalto-yliopiston sivuilta löydetyt CSP-otsakkeet.

4.6.1 Varmenteiden läpinäkyvyys

Varmenteiden läpinäkyvyys on prosessi, joka pyrkii lieventämään väärin myönnettyjen varmenteiden ongelmaa ylläpitämällä julkisia varmenne-lokeja, joista dataa ei voi poistaa, vaan niihin voi vain lisätä dataa. Lokit eivät itsessään estä väärinkäyttöä, mutta ne varmistavat, että asianomaiset, esimerkiksi varmenteiden haltijat, voivat havaita virheellisen myöntämisen. [28] Organisaatiot voivat valvoa tätä lokia ja saada ilmoitukset uusien varmenteiden rekisteröinnistä verkkotunnuksilleen.

Myös selaimet käyttävät näitä lokeja tarkastaakseen varmenteiden aitouden. Esimerkiksi Google Chrome vaatii uusien varmenteiden viemistä varmenne-lokeihin [6]. Muuten Chrome estää yhteyden ja esittää käyttäjälle

net::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED -virheen.

Hyökkääjä voi kuitenkin käyttää varmenteista kerättyä dataa verkkotunnusten keräämiseen. Varmenteiden lokeista voi hakea myös varmenteista löytyviä aliverkkotunnusten nimiä. Hakemalla lokeista "aalto.fi" termillä saadaan 621 erilaista verkkotunnusta.⁵ Hyökkääjä voisi käyttää näitä verkkotunnuksia porttiskannauksen kohteina ja etsiä haavoittuvia palveluita. Lisäksi verkkotunnuksista voi löytyä houkuttelevia kohteita palvelunestohyökkäyksille, kuten VPN-palveluihin viittaavia verkkotunnuksia.

⁵<https://crt.sh/?q=aalto.fi&exclude=expired&group=none>

```
220 smtp-out-01.aalto.fi ESMTP Sophos Email Appliance v4.5.3.6
250-smtp-out-01.aalto.fi
250-PIPELINING
250-SIZE 268435456
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

Kuva 6: Sähköpostiprotokollan otsakkeet.

5 Hakukoneet

Hakukoneet ovat tapa kartoittaa organisaation internetiin näkyvää hyökkäyspintaa. Julkisista hakukoneista löytyvät palvelut ovat haavoittuvimpia hyökkääjälle, koska ne ovat löydettävissä helpommin. Sivullaan Yhdysvaltojen kyberturvallisuusviranomaisen, Cybersecurity and Infrastructure Security Agency (CISA), neuvoo organisaatioita tarkkailemaan internetin hakukoneita aktiivisesti, jotta mahdolliset avoimet palvelut saadaan mahdollisimman nopeasti pois julkisista hakukoneista [8].

Tässä luvussa kerrotaan internetin hakukoneista ja vertaillaan niitä. Aiemmissä tutkimuksissa on käytetty internetin yleisempiä hakukoneita [30].

5.1 Esineiden internetin hakukone Shodan

Shodan on hakukone, joka on suunniteltu erityisesti löytämään ja indeksoimaan internetiin liitettyjä laitteita. Se on internetin laitteita indeksoivista hakukoneista tunnetuin. Toisin kuin perinteiset hakukoneet, jotka keskittyvät verkkosivujen indeksointiin, keskittyy Shodan erilaisten laitteiden, kuten palvelimien, reitittimien, webkameroiden, teollisuuden ohjausjärjestelmien ja IoT-laitteiden, indeksointiin. Suurin osa tiedoista saadaan palvelimen ja ohjelmistojen kertomista metatiedoista. Nämä voivat olla muun muassa tietoja palvelinohjelmistosta, mitä protokollaversioita palvelu tukee, tai tervetuloviesti. [61] [3]

Esimerkiksi hakemalla "aalto.fi" Shodanista löydetään avoin portti 25 IP-osoitteesta 130.233.228.120. Kuvassa 6 on esitetty Shodanin haulilla löydetyt palvelun otsakkeet. Otsakkeista nähdään muun muassa ulospäin suuntautuvan sähköpostiliikenteen osoite sekä sähköpostiohjelmiston versio.

Osoitteesta 130.233.248.118 löytyy webpalvelin (me310.org.aalto.fi), jossa on vanhentuneita ohjelmistoversioita käytössä. Vaikuttaa myös, että kyseisessä osoitteessa on vanha kurssisivu, jota on päivitetty viimeksi 16.4.2019. Tämä on hyvä esimerkki, miksi verkkoja tulisi kartoittaa suunnitelmallisesti ja usein. Hakutuloksissa näkyvää sivua tuskin käyttää kukaan aktiivisesti. Se lisää kuitenkin verkon hyökkäyspintaa, kun tiedetään, että palvelussa on todennäköisesti haavoittuvuuksia. Vaikka kyseinen palvelu itsessään ei olisi kovin tärkeä eikä sisältäisi suojattavaa tietoa, voi hyökkääjä

päästä sen kautta verkkoon sisään hyökkäämään muita laitteita vastaan eli laajentamaan vaikutusalueitaan, mitä kutsutaan lateraaliseksi laajentamiseksi. Hyökkääjä voi myös käyttää murrettua verkkosivua haittaohjelmien levittämiseen tai käyttää palvelinta palvelunestonhyökkäyksissä muihin kohteisiin. Shodanilla voi myös etsiä laitteita, joiden palvelinohjelmistoversioissa on haavoittuvuuksia.

Shodan osaa myös käänteisen DNS-haun, sekä SSL- ja TLS-varmenteiden tarkastuksen. Käänteisessä DNS-haussa etsitään IP-osoitteella sitä vastaava verkkotunnus. SSL- ja TLS-yhteyden tarkastamisessa muodostetaan yhteys porttiin, jolloin isäntälaitte esittää varmenteensa. Esitetystä varmenteesta voidaan selvittää erilaisia tietoja, kuten kenelle se on myönnetty.

5.2 Hyökkäyspinnan kartoittaja Censys

Censys on Shodanin tapaan hakukone ja tietokanta, jolla käyttäjä voi hakea internetiin kytkettyjä verkkolaitteita ja -palveluja.

Censys käyttää aktiivista skannausta, jossa se lähettää pyyntöjä eri IP-osoitteisiin ja analysoi saamansa vastaukset. Se skannaa internetiä käyttäen esimerkiksi ZMap ja ZGrab -työkaluja [29]. Censys käyttää ZMapia skannatakseen horisontaalisesti eli portti kerrallaan internetiä [11]. ZMapiin vastanneisiin portteihin se ajaa sovelluskohtaisia skanneja, esimerkiksi ZGrabin HTTP-protokollan tunnistuksen. Se kerää laitteiden tietoja avoimista porteista, protokollista, SSL- ja TLS-varmenteista sekä muista metatiedoista. Analysoimalla näitä tietoja käyttäjä voi arvioida laitteiden ja verkkojen turvallisuutta ja konfiguraatioita.

Censysin keräämät tiedot ovat saatavilla sen hakukoneesta, jonka avulla käyttäjät voivat etsiä tiettyjä laitteita, palveluja tai verkkotunnuksia. Sen avulla voidaan löytää laitteita, joilla on tiettyjä ominaisuuksia tai haavoittuvuuksia, tunnistaa väärin konfiguroituja järjestelmiä, valvoa SSL- ja TLS-varmenteiden kelpoisuutta sekä seurata teknologioiden käyttöä internetissä.

5.3 BinaryEdge-palvelu

BinaryEdge on *Platform as a Service* (PaaS) -palvelu, joka, on samankaltainen kuin Shodan, mutta sillä on muitakin ominaisuuksia, kuten tuki tietovuodon tunnistamiselle ja tuki kohdeverkkojen tunkeutumistestaukseen. [9] Se osaa myös seurata torrentien lataamista. Torrentit ovat tapa ladata ja levittää sisältöä vertaisverkossa. Torrenteissa on organisaatiolle oikeudellinen riski, koska niitä käytetään usein tekijänoikeuksilla suojatun materiaalin luvattomaan lataamiseen ja jakamiseen. Lisäksi niitä käytetään haittaohjelmien levitykseen. BinaryEdge kertoo torrentista muun muassa sen nimen, kategorian ja osoitteen, joka jakaa torrentia.

BinaryEdge laskee myös havainnolle riskiarvion. Riskiarvio lasketaan etäkäytön mahdollistavista palveluista, avoimista tietokannoista, heikosta salauksesta, torrenteista, haavoittuvuuksista ja avoimista porteista. [2] Muista hakukoneista ei löydy samanlaista riskiarviota, josta näkisi helposti palvelun mahdolliset tietoturvaongelmat. Niissä käyttäjä joutuu itse arvioimaan eri havaintojen vaikutusta palvelun tietoturvaan. BinaryEdge myös luetteli verkkotunnuksia, joten sillä voi hakea aliverkkotunnuksia.

```

HTTP/1.1 301 Moved Permanently
Date: Fri, 28 Apr 2023 08:38:37 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16
X-Powered-By: PHP/5.4.16
X-Redirect-By: WordPress
Location: https://me310.aalto.fi/
Content-Length: 0
Content-Type: text/html; charset=UTF-8

```

Kuva 7: HTTP-palvelun otsakkeet.

5.4 Hakukoneiden vertailu

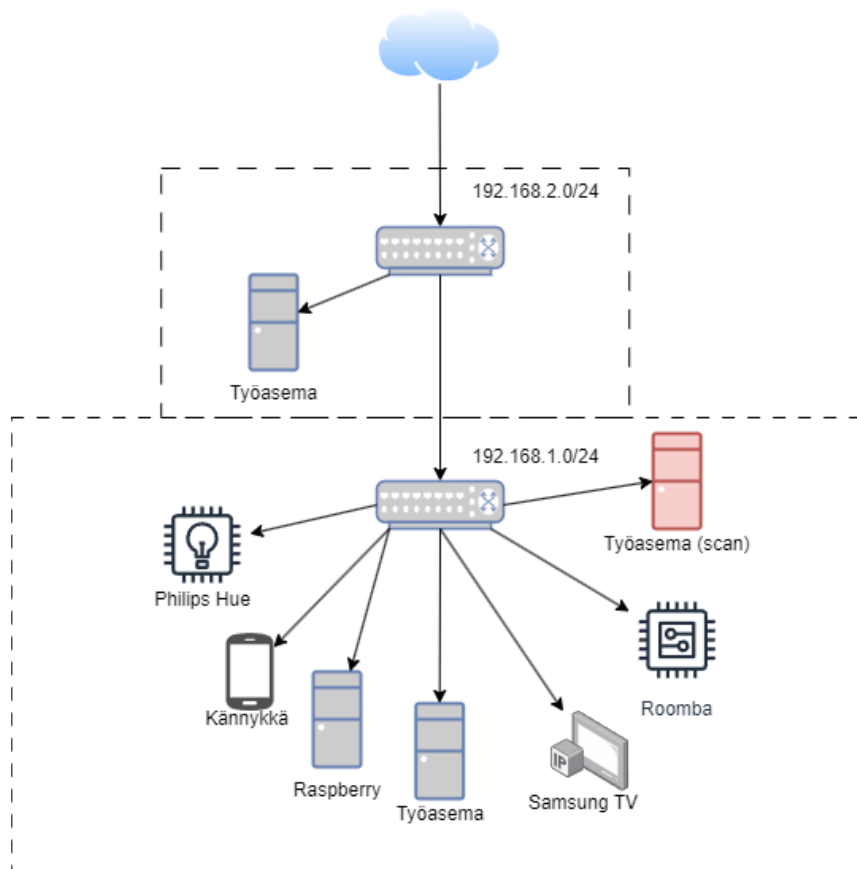
Työssä vertailtiin toiminnallisuuksiltaan viittä hakukonetta: Shodan, Censys, BinaryEdge, ZoomEye ja FOFA. Kaikissa skannaus oli melko tuore, ZoomEyen skanni oli vanhin, seitsemän päivää vanha. Jokainen palvelu palautti havaitusta palvelusta HTTP-otsakkeet, esimerkiksi Shodan tunnisti kuvan 7 mukaiset otsakkeet.

Taulukossa 2 on esitetty eri palveluiden ominaisuuksia. Palveluita vertailtiin CPE-tunnistuksen ja haavoittuvuuksien tunnistuksen perusteella. Huomattavaa on, että vaikka Censys tunnisti sivulta Apache-palvelimen, PHP-ohjelmiston sekä Linux Red Hatin CPE-arvot, ei se kuitenkaan listaa haavoittuvuuksia niille. Vaikka Censys ei listaa haavoittuvuuksia tuloksissa suoraan, on ne melko helppo etsiä haavoittuvuustietokannoista käyttämällä listattua CPE-arvoa [49].

Taulukko 2: Hakukoneiden vertailu taulukkona.

	Shodan	Censys	BinaryEdge	ZoomEye	FOFA
Ohjelmiston tunnistus (Apache)	ei	kyllä	kyllä	ei	ei
Sovellustunnistus (PHP)	ei	kyllä	ei	ei	ei
Haavoittuvuudet	kyllä ^a	ei	kyllä ^b	kyllä ^c	ei
Muuta	-	Koko datan saa ilmaiseksi ulos	Kertoo myös riskiarvion	Palauttaa sivun koko html:n	-

^a Löytää myös PHP:n haavoittuvuudet ^b Ei listaa haavoittuvuuksia ^c Ei PHP:n haavoittuvuuksia



Kuva 8: Testiverkko.

6 Testiverkon skannaus

Työn kokeellisessa osassa kartoitettiin testiverkkoa työssä esitellyillä työkaluilla. Kartoituksessa sovellettiin internetin laajuista skannausmenetelmää [44]. Työssä kartoitettiin koko porttiavaruus eli portit välillä 0-65535. Ensin kartoitettiin laajempi osa verkkoa masscannilla, jolla löydettiin laitteet, joissa oli avoimia portteja. Masscanin skanniin vastaaviin laitteisiin ajettiin Nmapilla porttiskannaus, jossa skannattavat portit saatiin masscannin tuloksista. Lopuksi masscannin skannaukseen vastaaviin portteihin ja laitteisiin suoritettiin vielä ZGrabin sovelluskohtaisia moduuleja, kuten HTTP-moduuli.

Kuvassa 8 on esitetty testiverkko. Testiverkossa on kaksi aliverkkoa. Verkon 192.168.2.0/24 reititin on yhteydessä internetiin ja on LAN-WAN -yhteydessä toiseen reitittimeen. Skannaus ajettiin verkosta 192.168.1.0/24, jossa on IoT-laitteita ja Windows-työasema. Palomuurit eivät salli yhteyttä verkon 192.168.2.0/24 työasemaan, joten sen ei pitäisi näkyä skannaustuloksissa.

Masscan löysi skannatuista verkoista 192.168.1.0/28 ja 192.168.2.0/28 uniikkeja portteja 25 kappaletta. Suurin osa havainnoista oli ennalta-arvattavia ja odotettuja, kuten Raspberryn SSH-palvelu ja web-palvelut. Toisaalta laitteista löytyi palveluita,

```
{
  "issuer_dn": "C=US, ST=Massachusetts,
    L=Beford, O=iRobot Corporation, OU=HBU, CN=Robot Intermediate CA A01",
  "validity": {
    "start": "2020-10-12T20:44:33Z",
    "end": "2030-10-13T20:44:33Z",
    "length": 315619200
  }
}
```

Kuva 9: Ote ZGrabin palauttamasta varmennedatasta.

joiden ei välttämättä tulisi olla päällä. Esimerkiksi Windows-työasemalta löytyi avoin portti 7680. Portin 7680 palvelu on Windowsin päivitysten jakopalvelu vertaisverkossa, jonka avulla Windows-laitteet samassa verkossa tai internetissä voivat ladata päivitykset Windows-laitteiden vertaisverkosta [40]. Lisäksi Samsungin televisiosta löytyi seitsemän avointa porttia.

Roomban robotti-imurista löytyi avoin portti 8883, jota se käyttää salattuun kommunikointiin pilven kanssa. ZGrabilla nähdään muun muassa Roomban varmennedatat. Kuvassa 9 on ote ZGrabin palauttamista varmennedatasta. Datasta nähdään varmenteen myöntäjä ja sen voimassaoloaika. Lisäksi siitä nähdään TLS-versio, jolla käsittely on tehty.

7 Vastakeinot tietoverkon kartoitukseen

Tämä luku kertoo erityyppisistä palomuuureista sekä verkkokaavioista. Luku kertoo myös niiden vaikutuksesta hyökkäyspintaan. Lisäksi luvun lopussa käydään läpi, miten palomuuureja yleensä käytetään organisaatioissa sekä niiden mahdollisia ongelmia.

7.1 Palomuurit

Palomuuuri on laitteisto, ohjelmisto tai molempien yhdistelmä, joka valvoo ja suodattaa verkkoliikennettä, joka liikkuu suojattuun verkkoon tai pois siitä. Se on työkalu, joka erottaa suojatun verkon tai sen osan suojaamattomasta verkosta, kuten internetistä. Määritelmän mukaan palomuuuri on siis työkalu, joka suodattaa sekä saapuvat että lähtevät paketit. [26]

7.1.1 Paketteja suodattavat palomuurit ja tilaton palomuuuri

Pakettien suodattamiseen tarkoitettut palomuurit ovat nopeita, koska niiden tekemät päätökset ovat logiikaltaan melko yksinkertaisia. Ne eivät pysty tarkastamaan pakettien sisältöä eli ne suodattavat IP-paketteja pelkästään otsakekenttien perusteella. Ne eivät myöskään tallenna mitään tilatietoja. Nämä palomuurit perustuvat lähde- ja kohde-IP-osoitteeseen, lähde- ja kohdeportin numeroon sekä protokollatyyppiin. [59]

Nämä palomuurit eivät ole kuitenkaan turvallisuuden kannalta optimaalisia, koska ne ohjaavat eteenpäin kaiken liikenteen, joka kulkee hyväksytyin portin kautta. Ne eivät siis pysty tunnistamaan yhteyden suuntaa. Näin ollen verkossa voi hyvinkin olla haitallista liikennettä, jos se vain pysyy hyväksyttävässä portissa. Tilattomat palomuurit eivät myöskään pysty havaitsemaan verkkopaketteja, joiden IP-osoitetiedot on väärennetty. Palomuuuri konfiguroidaan yleensä niin, että se pudottaa hiljaisesti kaikki paketit paitsi ne, jotka erikseen sallitaan. Koska paketit pudotetaan hiljaisesti, ei hyökkääjä saa mitään lisätietoa järjestelmästä.

7.1.2 Tilallinen palomuuuri

Tilallinen palomuuuri on verkon laitteisto tai ohjelmisto, joka on suunniteltu valvomaan ja hallitsemaan aktiivisten yhteyksien tilaa ja tekemään päätöksiä verkkoliikenteen sallimisesta kyseisten yhteyksien tilan perusteella. Tilalliset palomuurit pitävät kirjaa aktiivisten verkkoyhteyksien tilasta tilataulussa. Tauluun tallennetaan kunkin aktiivisen yhteyden ominaisuudet, kuten lähde- ja kohde-IP-osoitteet, lähde- ja kohdeportin numerot sekä yhteyden nykyinen tila. Tilallinen palomuuuri käyttää tätä taulua samaan yhteyteen kuuluvan verkkoliikenteen sallimiseksi. Se voi esimerkiksi sallia kaiken sisään tulevan liikenteen jo muodostetussa yhteydessä. [65]

Taulukossa 3 on esimerkki tilataulusta, joka kertoo yhteyden muodostuneen osoitteen 192.168.1.1 portista 49160 osoitteen 10.10.10.10 porttiin 80.

Taulukko 3: Palomuurin tilataulu.

Source Address	Source port	Destination Address	Destination Port	Connection State
192.168.1.1	49160	10.10.10.10	80	Established
192.168.1.2	49170	10.10.10.10	443	Established
192.168.1.3	49200	10.10.10.10	80	Established

7.1.3 Sovelluspalomuri

Web-sovellukseen voi hyökätä monin eri tavoin. Yleisimpiä ohjelmistojen heikkouksia ovat sivustojen välinen komentosarjahyökkäys (Cross-site scripting, XSS), erilaiset injektiot, erityisesti SQL-injektiot, käyttäjäsyötteen puutteellinen tarkastus ja sivuston rajat ylittävien pyyntöjen väärentäminen (Cross-site Request Forgery, CSRF) [42].

Injektioilla pyritään saamaan palvelin suorittamaan mielivaltaista koodia. Yksinkertaisimmillaan tällainen haavoittuvuus toimii, jos hyökkääjän toimittama parametri lisätään ennalta määritettyyn kyselyyn ja lähetetään kohdepalveluun tarkastamatta sitä. Ohjelmistoissa pitäisi tarkastaa tai hylätä kaikki sisältö, johon käyttäjä voi vaikuttaa.

CSRF-hyökkäyksessä hyökkääjän tavoitteena on saada kohde lähettämään tietämättään haitallinen verkkopyyntö sivustolle, johon kohde on kirjautuneena. Verkkopyyntö voidaan muotoilla siten, että se sisältää sopivia URL-parametreja, evästeitä ja muuta dataa, jotka näyttävät pyynnön käsittelevälle verkkopalvelimelle normaaleilta. Selaimen tallennetulla evästeellä kirjautunut käyttäjä voi tietämättään lähettää haitallisen HTTP-pyyntö sivustolle, joka käsittelee sen normaalisti. Sopivilla parametreilla voidaan saada käyttäjä esimerkiksi vaihtamaan salasanaa.

Sovelluspalomuri suojaa muun muassa näiltä hyökkäyksiltä. Se toimii internet-protokollapinon sovelluskerroksella. Vaikka sovelluspalomuri suojaa useilta sovelluskerroksen hyökkäyksiltä, on myös yleistä, että organisaatiot integroivat sen muihin tietoturvaratkaisuihin, kuten tunkeutumisen havaitsemisjärjestelmiin ja tunkeutumisen estojärjestelmiin.

Sovelluspalomuri sieppaa HTTP/S-pyyntöt, tarkastaa ne ja suodattaa haitalliset pyynnöt. Se tarkastaa myös palvelimen vastaukset ja etsii niistä tunnettuja web-sovellusten heikkouksia, kuten istunnon kaappausta, puskurin ylivuotoa, XSS:ää, viestintää komentopalvelimelle tai merkkejä palvelunestohyökkäyksistä. Se ei kuitenkaan suojaa nollapäivähyökkäyksiltä.

Koska yksityisyyden suoja ja tietoturva korostetaan yhä enemmän, on salauksen käytöstä tullut yleistä internetissä. Salaus takaa tietojen luottamuksellisuuden siirron aikana, mutta se on merkittävä haaste sovellustason palomuuereille. Sovellustason palomuri ei pysty tarkastamaan salatun viestinnän sisältöä, ellei sillä ole kykyä väärentää varmenteita ja purkaa viestintää. Jos palomuurille on annettu organisaatiossa juurivarmenne, joka mahdollistaa palvelinten varmenteiden väärentämisen, voi se olla viestinnän osapuolien välissä lukemassa ja analysoimassa viestintää, ja estää näin mahdollisia hyökkäyksiä.



Your connection is not private

Attackers might be trying to steal your information from **pinning-test.badssl.com** (for example, passwords, messages, or credit cards). [Learn more](#)

NET:ERR_SSL_PINNED_KEY_NOT_IN_CERT_CHAIN

Kuva 10: Virheilmoitus, kun selain ei luota kiinnitettyyn varmenteeseen.

Varmenteiden kiinnitys on suojausmekanismi, joka parantaa asiakkaan, kuten verkkoselaimen, ja palvelinten välisten TLS-yhteyksien luotettavuutta ja turvallisuutta. Perinteisessä varmenteen validointiprosessissa tarkistetaan, onko palvelimen varmenteen allekirjoittanut luotettava varmentaja. Kiinnitetty varmenne on erikseen liitetty sovellukseen, yleensä suoraan sen koodiin tai konfiguraatioon. Tällöin asiakasohjelmisto, kuten verkkoselain, luottaa yhteyteen vain, jos sille esitetty varmenne on sama kuin sovelluksen määrittelemä varmenne. Kuvassa 10 on esitetty selaimen virheilmoitus sen estettyä pääsyn sivustolle, koska kiinnitettyyn varmenteeseen ei luoteta. Jos sovellus käyttää varmenteiden kiinnitystä, ei palomuuuri voi purkaa viestintää, vaikka sillä olisi luotettu juurivarmenne. Selaimet käyttävät myös luvussa 4.6.1 mainittua varmennelokia tarkastaakseen varmenteen aitouden. Myös tämä vaikeuttaa ja monimutkaistaa sovelluspalomuurin toimintaa, sillä selaimet eivät lähtökohtaisesti luota palomuurin tarjoamaan varmenteeseen, joka ei ole varmennelokissa. Muuttamalla asetuksia voidaan selain konfiguroida luottamaan varmenteeseen, joka ei ole varmennelokissa. Asetuksia voidaan muuttaa myös keskitetysti organisaatioissa.

7.1.4 Kehittyneemmät palomuurit

Kehittyneimmissä palomuuureissa on kaikki perinteisten palomuurien ominaisuudet, kuten paketti-, verkko- ja porttisuodatus, osoitteiden kääntäminen, pakettien tilallinen tarkastus ja usein myös virtuaalinen yksityinen verkko (VPN). Siinä on myös kehittyneempiä ominaisuuksia, kuten tunkeutumisen estojärjestelmä, pakettien tarkastus ja käyttäjän tunnistaminen. Kehittyneemmät palomuurit pystyvät tunnistamaan ja valvomaan liikennettä sovelluksessa tarkastelemalla paketin sisältöä. Perinteiset palomuurit keskittyvät verkkoprotokolliin ja pakettien otsikkotietoihin. Sovellustietoisuus on tärkeä palomuurin ominaisuus. Se tarkoittaa, että palomuuuri pystyy tunnistamaan sovellukset portista ja protokollasta riippumatta, tunnistamaan käyttäjän ja identiteetin sekä paketin sisällön todellisen tarkoituksen. [31]

Kehittyneemmät palomuurin ominaisuudet vaativat lokien keräämistä pidemmältä ajalta, jotta palomuuuri tunnistaa poikkeavat tapahtumat oikein. Sen käyttöönotto ja hallitseminen voi olla monimutkaista erityisesti organisaatioissa, joilla ei ole omaa

kyberturvallisuusasiantuntemusta. Lisäksi kehittyneiden ominaisuuksien konfigurointi ja hienosäätö voi vaatia erityisosaamista.

7.1.5 Lokitus

Palomuurit lokittavat yleensä tapahtumia. Palomuurien lokienkäsittelyyn kuuluu tallentaa verkkotapahtumien tietoja, joista voi olla hyötyä muun muassa tietoturva-analyyseissa ja vianmäärityksessä. Ylläpitolokit sisältävät tietoja itse palomuurijärjestelmästä, kuten konfiguraatiomuutoksista ja järjestelmävirheistä. Niitä analysoimalla voidaan huomata mahdollinen tunkeutuminen itse palomuuriin. Turvallisuuslokitt keräävät tietoja yhteyksiin liittyvistä tapahtumista, kuten hyläystä tai sallitusta liikenteestä, tunkeutumisy yrityksistä ja muista tietoturvatapahtumista. Palomuurit lokittavat yleensä ainakin lähde- ja kohdeosoitteet, porttinumerot, protokollan sekä aikaleimat.

Palomuurin voi säätää hälyttämään epäilyttäviä tapahtumista tai estämään epäilyttävät laitteet kokonaan. Lokien analysoinnilla voidaan säätää kehittyneemmät palomuurit estämään tunkeutumisyrietykset automaattisesti. Lokien analysointia voidaan tehdä tapahtumien hallinta työkaluissa, jotka mahdollistavat useamman lokilähteen tietojen yhdistelyn ja korreloinnin. Keskitetyn lokienhallinnan käyttöönotto vaatii lokienhallintapolitiikan, josta selviää muun muassa, mitä lokitetaan ja mitä lokeilla tehdään. Lokitiedot pitäisi eriyttää muusta ympäristöstä ja varmuuskopioida. Niitä ei pitäisi myöskään päästä muokkaamaan.

7.1.6 Palomuurit organisaatioissa

Usein organisaatioissa käytetään useampaa kuin yhtä palomuuria. Organisaation verkon ulkorajalla voi olla yksinkertainen tilaton palomuuuri, joka estää kaikki ennalta määrittämättömiin portteihin tulevat yhteydet. Ennalta määritetyissä porteissa on usein palveluita, joita pitäisi pystyä käyttämään verkon yli, esimerkiksi VPN-palveluita tai web-sovelluksia. Tämä vähentää vahingossa paljastettujen palveluiden riskiä, sillä muista kuin ennalta määritetyistä porteista ei ole suoraa yhteyttä internetiin. Usein organisaation verkon sisälläkin käytetään palomuuureja. Esimerkiksi tietokantapalvelut suojataan, niin että vain tietyt palveluita tarvitsevat laitteet voivat käyttää niitä. Tämä suojaa tietokantoja mahdolliselta sisäverkosta tulevalta hyökkäykseltä.

Web-sovelluksissa taas voidaan käyttää sovelluspalomuuria, joka vähentää erilaisen injektiohyökkäysten riskiä. Sovelluspalomuurin konfigurointi toimimaan oikein TLS-salauksen kanssa on monimutkaista ja vaatii organisaation kaikkien käyttäjien kaikkien selainten asetusten konfigurointia [6]. Usean palomuurin ylläpitäminen vaatii lisäresursseja, koska niiden konfigurointi toimimaan yhdessä on haastavaa. Koska palomuurit ovat kalliita, käytetään yleensä yhtä reititykseen virtuaalisten verkkojen (VLAN) välillä. Palomuuureja voidaan käyttää myös yhteyksien estämiseen IP-osoitteen geolokaation perusteella, mikä voi auttaa palvelunestohyökkäyksien torjunnassa [34].

7.2 Verkkokaaviot

Verkkokaavio on visuaalinen kuvaus verkon arkkitehtuurista, komponenteista ja yhteyksistä. Se kuvaa miten eri laitteet, kuten tietokoneet, palvelimet, reitittimet, kytkimet ja muut verkkoyhteydelliset laitteet, on liitetty toisiinsa ja miten ne kommunikoivat toistensa kanssa verkossa.

Muun muassa ylläpitäjät ja systeemisuunnittelijat käyttävät verkkodiagrammeja verkkojen suunnittelemiseen, toteutukseen ja vianetsintään. Koska ne ovat visuaalisia, saa niistä helposti yleiskatsauksen verkon infrastruktuuriin. Verkkokaavio auttaa ymmärtämään laitteiden yhteyksiä toisiinsa, datan kulkua verkossa sekä verkon rakennetta.

Fyysinen verkkokaavio näyttää verkon muodostavien komponenttien, kuten kaapeleiden ja laitteistojen, fyysisen sijoittelun. Se hyödyntää yleensä rakennuksen pohjapiirrosta. Fyysisiä verkkokaavioita voidaan käyttää osana tilaturvallisuutta, kun esimerkiksi suunnitellaan palvelinten sijaintia rakennuksessa. Looginen verkkokaavio kuvaa verkon laitteiden yhteyksiä muihin verkon laitteisiin. Se kuvaa usein verkon aliverkot, IP-osoitteet ja verkkoprotokollat.

Verkkokaaviot tarjoavat visuaalisen esityksen verkkoinfrastruktuurista. Tämä visualisointi auttaa ymmärtämään verkon monimutkaisuutta ja laajuutta, mikä mahdollistaa paremman haavoittuvuuksien hallinnan. Kaaviot auttavat tunnistamaan erityistä tarkkailua vaativat kohteet. Analysoimalla verkkokaaviota asiantuntijat voivat tunnistaa mahdollisia haavoittuvuuspeisteitä ja voivat keskittyä kriittisten järjestelmien haavoittuvuuksien korjaamiseen tai muihin korkean riskin alueisiin.

Verkkokaavioiden avulla ylläpitäjät ja tietoturva-asiantuntijat voivat arvioida mahdollisia hyökkäysreittejä, joita hyökkääjä voi hyödyntää saadakseen luvattoman pääsyn järjestelmään tai vaarantaakseen järjestelmät. Hyökkäysreittien ymmärtäminen auttaa priorisoimaan haavoittuvuuksien korjaustoimia ja arvioimaan hyökkäyksen mahdollisia vaikutuksia. Verkkokaavioiden perusteella voidaan määrittää palomuurien, tunkeutumisen havaitsemisjärjestelmien tai muiden tietoturvakontrollien optimaalisen sijoittelu kriittisimpien laitteiden ja tietojen suojaamiseksi.

8 Hyökkäyspinnan minimointi

Tässä luvussa käydään läpi työkaluja hyökkäyspinnan minimointiin. Luvussa tutkitaan myös, miten minimointi vaikuttaa verkon tietoturvaan.

Säännölliset verkon skannaukset ja niiden perusteella tehtävät analyysit mahdollistavat uhkien havaitsemisen nopeasti. Siksi on tärkeää saada näkyvyys hyökkäyspintaan, jotta voidaan ehkäistä ongelmia verkkojen tietoturvan kanssa sekä varmistaa, että vain hyväksytyt laitteet pääsevät verkkoihin. Skannauksessa voidaan tunnistaa haavoituvuudet sekä mahdolliset konfiguraatiovirheet. Skannauksella voi myös tunnistaa palvelut, jotka ovat jo poistuneet käytöstä, mutta joita ei ole alas ajettu kunnolla.

Tarpeeton monimutkaisuus verkon käyttäjien hallinnassa sekä käytännöissä voi mahdollistaa verkkorikollisten luvattoman pääsyn yritystietoihin. Organisaatioilla tulisi olla prosessi, jolla poistetaan käytöstä tarpeettomat tai käyttämättömät ohjelmistot sekä laitteet verkon yksinkertaistamiseksi. Prosessin tulisi kattaa myös turhat käyttäjät ja liian laajat käyttöoikeudet. [35] Monimutkaiset järjestelmät voivat johtaa siihen, että käyttäjillä on pääsy resursseihin, joita he eivät käytä, mikä laajentaa hyökkääjän käytettävissä olevaa hyökkäyspintaa.

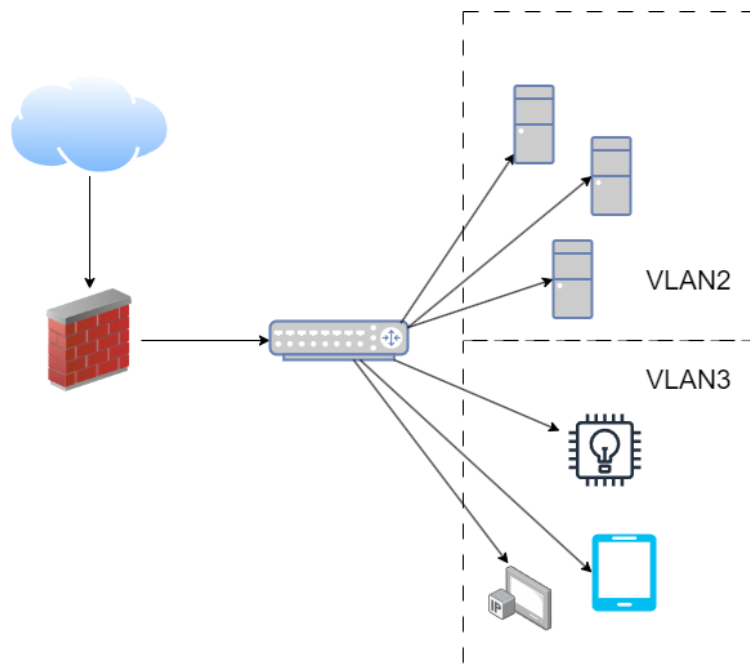
Täytyy kuitenkin muistaa myös, että työntekijät ovat tärkeässä osassa verkkohyökkäyksiä vastaan. Säännöllinen tietoturvallisuuskoulutus auttaa heitä ymmärtämään parhaat käytännöt ja havaitsemaan kalastelusähköpostien ja sosiaalisen manipuloinnin varoitusmerkit.

Nollaluottamus (zero trust) on kyberturvallisuuden käsite ja suunnittelutapa, jossa laitteisiin ei lähtökohtaisesti luoteta. Perinteinen tietoturvamalli perustuu oletukseen, että kaikkeen sisäverkon puolella luotetaan, kun taas mihinkään verkon ulkopuolella ei luoteta. Nollaluottamusmallissa sen sijaan validoidaan laite, vaikka se oltaisiin jo aiemmin todettu luotetuksi. Laitteille ja käyttäjille annetaan oikeuksia vain siksi ajaksi, kun he tarvitsevat niitä yksittäisiin tehtäviin. Näin oikeudet tarkistetaan usein, eikä vanhentuneita oikeuksia jää järjestelmään. [25] Eräs tapa noudattaa nollaluottamusmallia on segmentoida verkko, niin että verkon sisällä lateraalinen liikkuminen on hankalaa.

8.1 Verkon segmentointi

Verkon segmentoinnissa verkko jaetaan pienempiin, yleensä palomuuereilla eristettyihin segmentteihin tai aliverkkoihin turvallisuuden, suorituskyvyn ja hallittavuuden parantamiseksi. Näin verkon ylläpitäjät voivat hallita verkon liikennevirtaa aliverkkojen välillä yksityiskohtaisten sääntöjen perusteella. Verkon segmentoinnilla voidaan estää luvattomien käyttäjien pääsy käsiksi tärkeisiin omaisuuseriin, kuten asiakkaiden henkilökohtaisiin tietoihin tai yrityksen taloudellisiin tietoihin. [66] [39]

Eriytettyjen verkkojen laitteet eivät voi kommunikoida keskenään suoraan, mikä parantaa verkon tietoturvaa, koska jos toisessa verkossa on hyökkääjä, ei hän pysty hyökkäämään suoraan toisen verkon laitteisiin. Verkon segmentointi siis vaikeuttaa hyökkääjän lateraalista liikkumista. Lisäksi segmentointi tekee valvonnasta helpompaa ja helpottaa verkkomurtojen havaitsemista.



Kuva 11: Segmentoitu verkko.

Kuvassa 11 on esitetty segmentoitu verkko. Yhdessä verkossa on kaikki kriittisimmät laitteet, tässä tapauksessa työasemat. Se on esitetty kuvassa nimellä VLAN2. Toisessa verkossa (VLAN3) on muut vähemmän tärkeitä ja tietoturvaltaan heikommia laitteita. Jos siis VLAN3-verkon älytelevisio murretaan, ei hyökkääjä pääse vaarantamaan VLAN2-verkon työasemia. Oikein segmentoiduissa verkoissa hyökkääjä ei pysty liikkumaan, eikä siis pääse käsiksi toisen verkon tietoihin.

8.2 Palveluiden piilottaminen

Eräs tapa vähentää hyökkäysten todennäköisyyttä on paljastaa verkosta mahdollisimman vähän tai mahdollisesti väärentää tietoja, joita järjestelmä kertoo itsestään. Tutkimuksessa [16] listataan mahdollisiksi strategioiksi muun muassa versiotietojen väärentäminen, väärin tietojen lisääminen robots.txt -tiedostoon sekä väärin tiedostojen lisääminen web-palvelimelle. Samassa tutkimuksessa huomattiin, että robots.txt -tiedoston "disallow" polkua käytiin katsomassa, vaikka hakukoneiden ei pitäisi navigoida kyseiseen osoitteeseen.

Myös portteja voidaan piilottaa ja aktivoida ne vain, kun niitä tarvitaan. Piilottamiseen käytetään porttikoputus-tekniikkaa. Siinä portti pidetään suljettuna, kunnes tiettyihin portteihin otetaan oikeassa järjestyksessä yhteyttä. Kun oikeisiin portteihin lähetään sopivat paketit, avaa palomuuuri halutun portin hetkellisesti. Jos oikeassa sekvenssissä on useampi portti, on hyvin epätodennäköistä, että hyökkääjä onnistuu koputtamaan portteja oikeassa järjestyksessä. Porttikoputuksella onkin onnistuttu vähentämään epäonnistuneita kirjautumisyrittämiä SSH-palveluihin [1] [57].

9 Riskit

Järjestelmän tai verkon hyökkäyspinnan kartoittamatta jättäminen voi aiheuttaa useita riskejä, joiden myötä organisaatiot ovat alttiimpia erilaisille kyberturvallisuusuhkille. Hyökkäyspinnan kartoituksessa tunnistetaan ne kohdat, joissa hyökkääjä voi mahdollisesti hyödyntää haavoittuvuuksia. Tässä luvussa esitellään joitakin riskejä, jotka liittyvät järjestelmiin, joiden hyökkäyspintaa ei täysin tiedetä.

9.1 Tietovuodot

Hyökkääjien kohteena on usein tietokanta- ja sähköpostipalvelut, koska hyökkääjän on mahdollista löytää niistä mielenkiintoista tietoa itselleen. Datalla voi olla suoraan rahallista arvoa hyökkääjälle, kuten luottokorttitiedoilla. Jos data on organisaation kannalta kriittistä tai muuten suojattavaa, esimerkiksi terveystiedot, on sillä mahdollista kiristää organisaatiota maksamaan lunnaita datasta. Organisaatioiden tulisi varmuuskopioida kriittiset tiedot erilliseen järjestelmään. Varmuuskopioiden toimivuus tulisi myös tarkastaa säännöllisesti.

Tietomurron kohteeksi joutuminen voi aiheuttaa mainehaittaa organisaatiolle. Mainehaitan lisäksi organisaatio voi joutua maksamaan yleisen tietosuojasetuksen mukaisen sakon, jos ilmoitusta tietosuojaloukkauksesta ei ole tehty 72 tunnin sisällä tapahtuneesta, tai jos tietojen käsittely on ollut huolimaton.

9.2 Järjestelmän ja tiedon integriteetti

Tietomurron tutkinnassa selvitetään, mitä tietoturvaloukkauksessa tai verkkohyökkäyksessä on tapahtunut, mahdollistetaan hyökkääjän poistaminen järjestelmästä ja valmistaudutaan tietomurrosta toipumiseen. Tutkinta on vaativaa, joten pienet organisaatiot joutuvat yleensä ostamaan tutkinnan organisaation ulkopuolelta. Suuremmilla organisaatioilla voi olla oma tiimensä tietoturvaloukkausten käsittelyyn ja niiltä voi onnistua myös tietomurron tutkinta. Tietomurron varhainen havaitseminen on tärkeää, jotta niihin voidaan reagoida tehokkaasti. Havaitsemiseen voidaan käyttää esimerkiksi tunkeutumisen havaitsemisjärjestelmiä, tietoturvatietojen ja -tapahtumien hallintajärjestelmiä sekä päätelaitteiden havaitsemisjärjestelmiä. Niillä voidaan valvoa ja analysoida verkkoliikennettä, järjestelmälokeja ja muita asiaankuuluvia tietoja epäilyttävän toiminnan merkkien löytämiseksi. Yksinkertaisimmillaan organisaatio voi käyttää käyttöjärjestelmän omia järjestelmätyökaluja lokitukseen, esimerkiksi Microsoftin Sysmon-työkalulla saa tarkemmat lokit kuin Windowsin normaalilla tapahtumalokilla [32].

Etsimällä lokeista epätavallisia tapahtumia voidaan niistä löytää viitteitä hyökkääjistä. Tällaisia viitteitä ovat muun muassa epäilyttävä verkkoliikenne, luvattomat kirjautumisyritykset ja tiedostojen tiivisteet.

- **Epäilyttävä verkkoliikenne**

Lokeissa voi näkyä epäilyttäviä portteja tai osoitteita. IP-osoitteet voivat sijaita maissa, joihin ei yleensä ole liikennettä. Lisäksi liikennettä voi olla normaalia

enemmän, erityisesti lähetyliikenteen suuri määrä voi viitata tietojen varastamiseen.

- **Kirjautumisyrietykset**

Lokeissa voi olla luvattomia kirjautumisyrietyksiä normaalia enemmän. Kirjautumisyrietykset voivat myös onnistua, jos hyökkääjä on onnistunut kalastelemaan tunnukset aiemmin.

- **Tiedostojen tiivistet**

Lokeissa voi näkyä tunnettujen haittaohjelmien tiedostotiivistettä.

Vaikka mahdollisesta hyökkäyksestä ei aiheutuisi suoria menetyksiä tai tietovuotoa, aiheuttaa sen selvittäminen kuitenkin kustannuksia. Tietomurron tutkinta voi olla kallista ja vie aikaa, jos sitä ei ole suunniteltu tai huomioitu aiemmin organisaation prosesseissa. Tietoturvaloukkaukset voivat häiritä organisaation toimintaa, jos palveluita joudutaan ottamaan pois käytöstä ja oikeiden käyttäjien pääsy järjestelmään estyy. Tietoturva-aukkojen korjaaminen sekä järjestelmien ja tietojen palauttaminen vaatii lisätyötä. Samalla voidaan menettää jo tehtyä työtä, jos varmuuskopiot eivät ole tarpeeksi tuoreita. Lisäksi hyökkääjän karkotus pitää tehdä huolella, jotta järjestelmään ei jää hyökkääjän asentamia takaportteja, joista voi päästä uudelleen järjestelmään.

9.3 Palvelunestohyökkäys

Palvelunestohyökkäys on yleisnimitys hyökkäykselle, jossa käytetään palvelimen resursseja niin paljon, että oikeiden käyttäjien pääsy järjestelmään estyy tai järjestelmän käyttö hidastuu merkittävästi. Palvelunestohyökkäykset ovat usein hajautettuja eli verkkoliikenne tulee useasta eri verkkolaitteesta, jolloin yksittäisten IP-osoitteiden estäminen ei auta hyökkäyksen torjunnassa. Hajautettujen hyökkäysten taustalla on usein hyökkääjän bottiverkko, jolla hyökkääjä saa jaettu liikenteen useammalle laitteelle. Palvelunestohyökkäykset eivät vaadi laajaa teknistä osaamista, koska niitä voi ostaa palveluina verkosta. [34]

9.3.1 Peilaava sekä vahvistettu palvelunestohyökkäys

Peilaavassa palvelunestohyökkäyksessä lähetetään UDP-pyyntöpaketti ulkopuoliselle palvelimelle, mutta lähde-IP-osoite väärennetään kohdepalvelimen IP-osoitteeksi. Ulkopuolinen palvelin lähettää vastauksen hyökkääjän kohdepalvelimelle, koska se luulee, että pyyntö tuli sieltä. Jos vastaus on suurempi kuin pyyntö tapahtuu peilaavassa hyökkäyksessä myös vahvistus, jolloin kohdepalvelin vastaanottaa enemmän liikennettä kuin hyökkääjä lähettää ulkopuoliselle palvelimelle. Joissain protokollissa vahvistuskerroin voi olla merkittävä, esimerkiksi hyökkääjän 1 Mt/s liikenne BACnet-protokollan palvelimeen voi reflektoitua 120 Mt/s liikenteeksi kohdepalvelimelle [18]. Peilaavassa hyökkäyksessä hyökkääjä saa myös piilotettua oman IP-osoitteensa kohdejärjestelmältä.

9.3.2 Volumetriset hyökkäykset

Volumetrisessä hyökkäyksessä jumiutetaan kohteen verkkoyhteys. Siinä lähetetään niin paljon paketteja, että kohteen verkkoyhteys jumiutuu. Volumetrisessä hyökkäyksessä voivat kärsiä myös muut palvelut, jotka käyttävät samaa verkkoyhteyttä.

Volumetrisen hyökkäyksen lisäksi voidaan käyttää vastakkaista logiikkaa eli lähettää pyyntöjä mahdollisimman hitaasti. *Slowloris*-hyökkäys toimii luomalla useita yhteyksiä verkkopalvelimeen [62]. Jokaisessa yhteydessä lähetetään pyyntö, joka ei sisällä sitä päättävää rivinvaihtoa. Hyökkääjä lähettää säännöllisesti lisää dataa pitääkseen yhteyden elossa, mutta ei koskaan lähetä lopettavaa rivinvaihtoa. Verkkopalvelin pitää yhteyden auki odottaen lisädataa. Hyökkäyksen jatkuessa *Slowloris*-yhteyksien määrä kasvaa, ja lopulta kaikki käytettävissä olevat verkkopalvelinyhteydet loppuvat, jolloin verkkopalvelin ei pysty vastaamaan muihin pyyntöihin.

Klassinen palvelunestohyökkäys on TCP SYN -tulvahyökkäys, jossa puolittain avoimet yhteydet vievät resursseja palvelimelta, eivätkä oikeat käyttäjät voi käyttää palvelua [34]. Puolittain avoimet yhteydet joutuvat odottamaan aikakatkaisua, jotta ne sulkeutuvat. Mikäli hyökkääjä luo jatkuvasti uusia yhteyksiä voi palvelimen käyttö estyä pitkäksi ajaksi. Hyökkääjä voi myös kuluttaa palvelimen resurssit loppuun, esimerkiksi luomalla vaativia tietokantakyselyitä, jolloin tietokantapalvelimelta voi loppua prosessointiteho. Prosessointitehon loppuessa tietokantapalvelin ei voi enää käsitellä tietokantakyselyitä ja palvelun käyttö hidastuu tai estyy kokonaan. Palvelun estyminen saattaa onnistua myös hyväksikäyttämällä haavoittuvuuksia, esimerkiksi HTTP/2-protokollaan julkaistiin haavoittuvuus (CVE-2023-44487), jonka avulla voitiin kuluttaa palvelimen resurssit loppuun.

9.3.3 Palvelunestohyökkäykset organisaatiossa

Palvelunestohyökkäyksen riskiä voi pienentää pitämällä organisaation sisäiset palvelut vain sisäverkossa. Tällöin palvelut eivät ole saavutettavissa suoraan internetistä, eivätkä ne ole alttiita internetistä tuleville palvelunestohyökkäyksille. Kun liikenne salataan ja reititetään VPN-palvelimen kautta, voi palvelin toimia puskurina suodattaen haitallisen liikenteen pois ennen kuin se saavuttaa kohdeverkon. Organisaation sisäverkon palveluiden etäkäyttö onnistuu VPN-yhteyden avulla. VPN-palvelin voi joutua palvelunestohyökkäyksen kohteeksi, mutta sisäverkon palvelut toimivat silti sisäverkossa. Myös pilvipalveluina toteutetut organisaation sisäiseen käyttöön tarkoitetut palvelut voidaan suojata VPN:llä. Lisäksi VPN voidaan suojata palomuurilla, jotta se toimii paremmin myös palvelunestohyökkäystilanteissa.

Hyökkääjä voi yrittää selvittää organisaation VPN-palvelimen osoitteita esimerkiksi etsimällä sertifikaattilokeista niihin viittaavia verkkotunnuksia. VPN-palvelimet voivat olla houkuttelevia kohteita palvelunestohyökkäyksille, koska ne ovat tärkeä osa organisaation tietoverkkorakenteessa. Jos hyökkääjä kohdistaa palvelunestohyökkäyksen VPN-palvelimeen, voi se mahdollisesti käyttää palvelimen resurssit loppuun ja aiheuttaa käyttökatkoksia kaikille palvelimeen yhdistetyille käyttäjille ja palveluille. Tämä voi aiheuttaa merkittävää haittaa etenkin etätyöntekijöille, sillä he eivät välttämättä voi työskennellä ilman yhteyttä organisaation verkkoon. Jos organisaatiossa on

pakotettu VPN-yhteys kaikelle liikenteelle, reitittyy kaikki liikenne VPN-yhteyden kautta. Tällöin VPN-palvelun ollessa tavoittamattomissa estyy käyttäjien pääsy internetiin kokonaan, sillä laitteilla ei ole reittiä internetiin.

Vaikka palvelunestohyökkäyksiä ei voi kokonaan estää, voi niiden vaikutuksia vähentää huomattavasti. Tunnistamalla haavoittuvimmat ja tärkeimmät palvelut voidaan niitä suojata paremmin. Niiden löytämiseen voidaan käyttää luvussa 4 esiteltyjä työkaluja. Avoimia ja haavoittuvia palveluita voidaan käyttää hyväksi palvelunestohyökkäyksissä. Organisaation IP-osoitteita saatetaan myös estää, jos se osallistuu palvelunestohyökkäyksiin. Palveluja voidaan suojata palvelunestohyökkäyksiä vastaan palomuuureilla, joita on esitelty luvussa 7.1.

10 Pohdinta

Tässä luvussa arvioidaan työssä käsiteltyä hyökkäyspinnan kartoitusmenetelmää sekä arvioidaan testiverkon kartoituksen tuloksia. Lisäksi tässä luvussa arvioidaan tutkimuksen rajoitteita sekä esitetään ideoita jatkotutkimukseen.

Hyökkäyspinnan analyysi on kriittinen osa kyberturvallisuusriskien ymmärtämistä ja niiden vähentämistä. Tässä työssä on perehdytty eri tekijöihin, jotka vaikuttavat järjestelmän tai verkon haavoittuvuuteen. Hyökkäyspinta on kaikkien niiden rajapintojen summa, joista hyökkääjä voi yrittää päästä järjestelmään tai verkkoon. Hyökkäyspinnan ymmärtäminen on siis tärkeä osa organisaation tietoturva.

Yksi työn tärkeimmistä huomioista on hyökkäyspinnan dynaaminen luonne. Hyökkäyspinta muuttuu aina, kun otetaan lisää palveluita käyttöön tai kun muutetaan organisaation infrastruktuuria. Hyökkäyspinta laajenee, kun uusia ominaisuuksia otetaan käyttöön ja olemassa olevat järjestelmät kytkeytyvät toisiinsa monimutkaisilla tavoilla. Hyökkäyspintaa tulisi kartoittaa jatkuvasti, jotta mahdolliset ongelmat saadaan korjattua nopeasti. Hyökkäyspinnan hallintaan onkin viime aikoina tullut useampia kaupallisia tuotteita, joiden ominaisuudet vaihtelevat kevyistä kartoituksista digitaalisen toimitusketjun valvontaa. Samoissa tuotteissa on usein myös palomuurien ominaisuuksia.

Luvussa 6 kokeiltu tapa skannata verkkoa sisäpuolelta käsin havaittiin toimivaksi tavaksi kartoittaa hyökkäyspintaa. Samaa tapaa voidaan kuitenkin käyttää myös skannaamiseen verkon ulkopuolelta, jolloin joudutaan usein hakemaan hyväksyntä verkon omistajalta, jos organisaatio ei itse omista verkkoa. Skannaus tunnisti oikein muun muassa laitteissa olevat SSH- ja webpalvelut. Skannatuista laitteista löytyi myös avoimia portteja ja palveluita, joiden olisi pitänyt olla kiinni. Ennustettavasti älytelevisiosta löytyi useampi avoin portti. Älytelevisioissa on paljon erilaisia ominaisuuksia ja palveluita, jotka vaativat avoimia portteja, jotta laite voi kommunikoida oikein muiden verkon laitteiden kanssa. Toisaalta nämä ominaisuudet lisäävät koko verkon hyökkäyspintaa, koska hyökkääjä voi päästä murtamaan kyseiset palvelut ja mahdollisesti levittäytymään muihin verkon laitteisiin. Ylimääräiset ja käyttämättömät palvelut tulisi kytkeä pois päältä tai asettaa palomuuuri estämään liikenne kyseisiin palveluihin.

Myös viranomaiset kartoittavat hyökkäyspintaa, esimerkiksi Ison-Britannian kyberturvallisuusviranomainen (National Cyber Security Centre, NCSC) skannaa Ison-Britannian verkkoja. Viranomaisten skannaukset auttavat ymmärtämään maan järjestelmien haavoittuvuuksia ja turvallisuutta. Kartoitukset auttavat myös omistajia ymmärtämään järjestelmiensä turvallisuutta, koska tietoa jaetaan yleensä myös heille. Lisäksi ne nopeuttavat viranomaisten reagointia häiriötilanteisiin, kuten laajasti hyödynnettyihin nollapäivähaavoittuvuuksiin. [46]

NCSC:llä on myös *Early Warning* -niminen järjestelmä, johon organisaatiot voivat syöttää IP-osoitteensa ja verkkotunnuksensa. Järjestelmä lähettää hälytyksen yhteyshenkilölle, jos organisaation verkossa näkyy viitteitä hyväksikäytöstä. Järjestelmä kertoo yhteyshenkilölle myös haavoittuvista palveluista tai mahdollisesti väärin konfiguroiduista palveluista, joiden ei tulisi näkyä internetiin, kuten avoimista tietokannoista. [45] Suomessa on samankaltainen palvelu *Hyöky - kansallinen*

hyökkäyspintakartoitus, joka on kohdennettu kunnille ja muille julkishallinnon organisaatioille [36]. Viranomaiset ovat tunnistaneet tarpeen helposti käyttöönotettaville kyberturvallisuuspalveluille, joilla organisaatiot voivat parantaa tietoturvaansa ilman suuria investointeja.

Hyökkäyspinta ylettyy muuallekin kuin organisaation omaan verkkoon. Työssä esitellyllä metodilla ei saa kovin laajaa kuvaa muun muassa pilvipalveluiden hyökkäyspinnasta, koska skannausta ei voi suorittaa samalla tavalla pilvipalveluihin. Verkkotunnusten listauksella on kuitenkin mahdollista saada hieman näkyvyyttä myös organisaation verkon ulkopuolella oleviin palveluihin. Työssä käytetty metodi vie myös huomattavasti enemmän aikaa IPv6-verkoissa, jos ei ole tietoa laitteiden IPv6-osoitteista läpi käytävän osoiteavaruuden pienentämiseksi.

Työssä toteutettu kartoitus toimi hyvin IPv4-verkkoon. Työssä käsiteltiin kuitenkin vain lyhyesti IPv6-verkkoja. Jatkotutkimuksessa olisi hyvä käydä niitä tarkemmin läpi. Jatkotutkimuksessa voisi käydä myös läpi pilvipalveluiden hyökkäyspinnan kartoitusta.

Kun organisaatiot pyrkivät löytämään tasapainon toiminnallisuuden ja turvallisuuden välille, tulee hyökkäyspinnan kartoituksen ja analyysin rooli yhä keskeisemmäksi. Hyökkäyspinnan kattava ymmärtäminen ja seuraaminen on olennainen osa verkon tietoturvaa, sillä verkon nopeasti muuttuvassa uhkakuvassa on tärkeää löytää mahdolliset haavoittuvuudet nopeammin kuin hyökkääjä.

11 Yhteenveto

Työn tarkoituksena oli luoda laaja kokonaiskatsaus hyökkäyspintaan käsitteenä sekä selvittää menetelmiä hyökkäyspinnan kartoittamiseen tietoverkoissa. Työssä määritettiin hyökkäyspinta tarkoittamaan niiden järjestelmän rajapintojen joukkoa, joiden kautta mahdollinen hyökkääjä voi päästä järjestelmään sisään, löytää haavoittuvuuksia ja vahingoittaa sitä tai muuttaa sen toimintaa.

Tässä tutkielmassa esitellyillä menetelmillä on mahdollista kartoittaa organisaation hyökkäyspintaa verkossa. Työssä esitellyillä skannaustyökaluilla voi kartoittaa organisaation tietoverkkoa myös sisäverkosta. Listaamalla verkkotunnuksia voidaan hyökkäyspinnan kartoitus laajentaa myös julkisiin verkkoihin. Internetin laitteiden löytämiseen tarkoitetuilla hakukoneilla voi myös luoda nopean katsauksen organisaation ulospäin näkyvään hyökkäyspintaan.

Soveltamalla näitä tekniikoita jatkuvasti organisaatiot saavat kokonaisvaltaisen käsityksen hyökkäyspinnastaan, ja voivat priorisoida ja toteuttaa tehokkaampia turvatoimia. Tehokkaimpia toimia on vähentää hyökkäyspintaa sulkemalla turhia palveluita ja piilottaa tärkeimmät palvelut VPN:n taakse. Lisäksi palvelut tulisi suojata palomureilla asianmukaisesti. Tämä ennakoiva asenne ei ainoastaan paranna yleistä tietoturvaa vaan auttaa myös tietoon perustuvassa riskienhallinnassa.

Työssä skannattiin testiverkkoa noudattamalla internetin laajuisten skannausten metodologiaa. Verkko skannattiin ensin nopeammalla asynkronisella työkalulla, minkä jälkeen havaitut laitteet skannattiin tarkemmin Nmap- ja ZGrab-työkaluilla. Testiverkosta löytyi yllättäviä havaintoja. Osa porteista oli auki, vaikka niiden olisi pitänyt olla kiinni. Havainnot vahvistavat käsitystä, että hyökkäyspintaa tulisi kartoittaa jatkuvasti.

Lähteet

Viitteet

- [1] Antonios S Andreatos. Hiding the SSH port via smart port knocking. In *The 2017 International Conference on Circuits, Systems, Signal Processing, Communications and Computers*, 2017.
- [2] BinaryEdge. BinaryEdge. <https://www.binaryedge.io/data.html>, 2023.
- [3] Roland C. Bodenheim. Impact of the Shodan computer search engine on internet-facing industrial control system devices, 2014. <https://scholar.ait.edu/etd/590/>.
- [4] Elias Bou-Harb, Mourad Debbabi, and Chadi Assi. Cyber scanning: a comprehensive survey. *IEEE Communications Surveys & Tutorials*, 16(3), 2013.
- [5] Brian E. Carpenter, Tim Chown, Fernando Gont, Sheng Jiang, Alexandre Petrescu, and Andrew Yourtchenko. Analysis of the 64-bit Boundary in IPv6 Addressing. RFC 7421, 2015.
- [6] Chromium Source Repository. Certificate Transparency. <https://chromium.googlesource.com/chromium/src/+master/net/docs/certificate-transparency.md>, 2024.
- [7] Michelle Cotton, Lars Eggert, Dr. Joseph D. Touch, Magnus Westerlund, and Stuart Cheshire. Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry. RFC 6335, 2011.
- [8] Cybersecurity and Infrastructure Security Agency - CISA. Stuff Off Search. <https://www.cisa.gov/resources-tools/resources/stuff-search>, 2021.
- [9] Artjoms Daskevics and Anastasija Nikiforova. ShoBeVODSDT: Shodan and Binary Edge based vulnerable open data sources detection tool or what Internet of Things Search Engines know about you. In *2021 second international conference on intelligent data science technologies and applications (IDSTA)*. IEEE, 2021.
- [10] Debian manpages archive. Services – internet network services list. <https://manpages.debian.org/bookworm/manpages/services.5.en.html>, 2023.
- [11] Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J Alex Halderman. A search engine backed by Internet-wide scanning. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015. ACM.

- [12] Zakir Durumeric, Eric Wustrow, and J Alex Halderman. ZMap: Fast internet-wide scanning and its security applications. In *22nd USENIX Security Symposium*, 2013.
- [13] Clément Elbaz, Louis Rilling, and Christine Morin. Fighting N-day vulnerabilities with automated CVSS vector prediction at disclosure. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*. Association for Computing Machinery, 2020.
- [14] FIRST (Forum of Incident Response and Security Teams). CVSS Specification Document. <https://www.first.org/cvss/specification-document>, 2023.
- [15] FIRST (Forum of Incident Response and Security Teams). CVSS user guide. <https://www.first.org/cvss/user-guide>, 2023.
- [16] Daniel Fraunholz and Hans D Schotten. Defending web servers with feints, distraction and obfuscation. In *2018 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2018.
- [17] Oliver Gasser. *Evaluating network security using Internet-wide measurements*. PhD thesis, Technische Universität München, 2019.
- [18] Oliver Gasser, Quirin Scheitle, Carl Denis, Nadja Schricker, and Georg Carle. Security implications of publicly reachable building automation systems. In *2017 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2017.
- [19] Elizabeth Chaos Golubitsky. *Measuring Attack Surfaces of Open Source IMAP Servers*. PhD thesis, Carnegie Mellon University. Information Networking Institute, 2005.
- [20] Fernando Gont and Tim Chown. Network Reconnaissance in IPv6 Networks. RFC 7707, 2016.
- [21] Robert David Graham. masscan. <https://github.com/robertdavidgraham/masscan>, 2023.
- [22] Michael Howard, Jon Pincus, and Jeannette M. Wing. Measuring relative attack surfaces. In *Computer Security in the 21st Century*. Springer-Verlag.
- [23] Internet Assigned Numbers Authority (IANA). Service name and transport protocol port number registry. <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>, 2023.
- [24] Patrik Karlsson. Nmap MySQL-empty-password. <https://github.com/nmap/nmap/blob/master/scripts/mysql-empty-password.nse>, 2023.

- [25] John Kindervag et al. Build security into your network's DNA: The zero trust network architecture. *Forrester Research Inc*, 27, 2010.
- [26] Joseph Migga Kizza, Wheeler Kizza, and Wheeler. *Guide to computer network security*, volume 8. Springer, 2013.
- [27] Sumit Kumar and Sithu D Sudarsan. An innovative UDP port scanning technique. *International Journal of Future Computer and Communication*, 3(6), 2014. IACSIT Press.
- [28] Ben Laurie, Adam Langley, Emilia Kasper, Eran Messeri, and Rob Stradling. Certificate Transparency Version 2.0. RFC 9162, 2021.
- [29] Seungwoon Lee, Seung-Hun Shin, and Byeong-hee Roh. Abnormal behavior-based detection of Shodan and Censys-like scanning. In *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 2017.
- [30] Ruiguang Li, Meng Shen, Hao Yu, Chao Li, Pengyu Duan, and Lihuang Zhu. A survey on cyberspace search engines. In *Cyber Security: 17th China Annual Conference, CNCERT 2020, Beijing, China, August 12, 2020, Revised Selected Papers 17*. Springer Singapore, 2020.
- [31] Junyan Liang and Yoohwan Kim. Evolution of firewalls: Toward securer network using next generation firewall. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2022.
- [32] Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. *Opas tietomurtojen havaitsemiseen*. 2020. <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Opas-tietomurtojen-havaitsemiseen.pdf>.
- [33] Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. *Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2020*. Traficom julkaisu 5/2021, 2021.
- [34] Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. *Palvelunestohyökkäys – Toimintaohje*. Traficom julkaisu 25/2022, 2022.
- [35] Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. *Toimintaohje – Pilviympäristöjen poikkeamanhallinta*. Traficom julkaisu 18/2023, 2023.
- [36] Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. *Hyöky*, 2024. <https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilan-nekuva-ja-verkostojohtaminen/hyoky>.
- [37] Pratyusa K Manadhata, Kymie MC Tan, Roy A Maxion, and Jeannette M Wing. An approach to measuring a system's attack surface. Technical report, Carnegie Mellon University, School of Computer Science, 2007.

- [38] Pratyusa K Manadhata and Jeannette M Wing. Measuring a system's attack surface. Technical report, Carnegie Mellon University, School of Computer Science, 2004.
- [39] Neerja Mhaskar, Mohammed Alabbad, and Ridha Khedri. A formal approach to network segmentation. *Computers & Security*, 2021. Elsevier.
- [40] Microsoft. Windows as a Service (WaaS) Delivery Optimization FAQ. <https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-faq>, 2023.
- [41] MITRE. MITRE ATT&CK Tactics. <https://attack.mitre.org/tactics>, 2024.
- [42] MITRE - Common Weakness Enumeration (CWE). Top 25 most dangerous software weaknesses. https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html, 2023.
- [43] Mozilla Developer Network (MDN). Content Security Policy (CSP). <https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>, 2023.
- [44] David Myers, Ernest Foo, and Kenneth Radke. Internet-wide scanning taxonomy and framework. In *Proceedings of the 13th Australasian Information Security Conference (AISC 2015)*. Australian Computer Society, 2015.
- [45] National Cyber Security Centre (NCSC). Early Warning. <https://www.ncsc.gov.uk/information/early-warning-service>. 2021.
- [46] National Cyber Security Centre (NCSC). NCSC Scanning information. <https://www.ncsc.gov.uk/information/ncsc-scanning-information>. 2022.
- [47] National Institute of Standards and Technology (NIST) - CSRC. Common Platform Enumeration (CPE). <https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/cpe>, 2023.
- [48] National Vulnerability Database (NVD) - NIST. CVSS - Common Vulnerability Scoring System. <https://nvd.nist.gov/vuln-metrics/cvss>, 2023.
- [49] National Vulnerability Database (NVD) - NIST. NVD - Common Platform Enumeration (CPE) Search. <https://nvd.nist.gov/products/cpe/search>, 2023.
- [50] Nmap organization. Host discovery. <https://nmap.org/book/man-host-discovery.html>, 2023.
- [51] Nmap organization. Port specification. <https://nmap.org/book/man-port-specification.html>, 2023.

- [52] Nmap organization. UDP scan. <https://nmap.org/book/scan-methods-udp-scan.html>, 2023.
- [53] Nmap organization. Version detection. <https://nmap.org/book/man-version-detection.html>, 2023.
- [54] Nmap organization. Nmap services file. <https://svn.nmap.org/nmap/nmap-services>, 2024.
- [55] Samson O Oruma, Mary Sánchez-Gordón, Ricardo Colomo-Palacios, Vasileios Gkioulos, and Joakim K Hansen. A systematic review on social robots in public spaces: Threat landscape and attack surface. *Computers*, 11(12), 2022. MDPI.
- [56] Ondrej Pospisil, Petr Blazek, Radek Fujdiak, and Jiri Misurec. Active scanning in the industrial control systems. In *2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC)*. IEEE, 2021.
- [57] Jigar A Raval and Samuel Johnson. Port Knocking—An Additional Layer of Security for SSH and HTTPS. In *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, 2013.
- [58] Ronald S Ross. *Guide for conducting risk assessments*. NIST Special Publication, 2012.
- [59] Derrick Rountree. *Security for Microsoft Windows system administrators: introduction to key information security concepts*. Elsevier, 2011.
- [60] SANS Institute. SANS Internet Storm Center. <https://isc.sans.edu/top10.html>. 2024.
- [61] Shodan. What is Shodan. <https://help.shodan.io/the-basics/what-is-shodan>, 2024.
- [62] William Stallings, Lawrie Brown, Michael D Bauer, and Michael Howard. *Computer security: principles and practice*, volume 2. Pearson Upper Saddle River, 2012.
- [63] Mark Stamp. *Information security: principles and practice*. John Wiley & Sons, 2011.
- [64] Sal Stolfo, Steven M Bellovin, and David Evans. Measuring security. *IEEE Security & Privacy*, 9(3), 2011.
- [65] John Wack, Ken Cutler, and Jamie Pole. Guidelines on firewalls and firewall policy. *NIST special publication*, 800, 2002.

- [66] Neal Wagner, Cem Ş Şahin, Michael Winterrose, James Riordan, Jaime Pena, Diana Hanson, and William W Streilein. Towards automated cyber decision support: A case study on network segmentation for security. In *2016 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE, 2016.
- [67] Mengyuan Zhang, Lingyu Wang, Sushil Jajodia, and Anoop Singhal. Network attack surface: Lifting the concept of attack surface to the network level for evaluating networks' resilience against zero-day attacks. *IEEE Transactions on Dependable and Secure Computing*, 2018.
- [68] ZMap Project. ZGrab. <https://github.com/zmap/zgrab2>, 2023.
- [69] ZMap Project. ZMap: the internet scanner. <https://github.com/zmap/zmap>, 2023.