Nimi: _____ Päivämäärä: _____ Pisteet: _____

Pimeä verkko vs. syvä verkko: turvallisuus ja Erot

Hakukoneindeksointi, syvän verkon tietokannat, Tor-sipulireititys, verkon anonymiteetti ja riskit

DARK WEB VS. DEEP WEB: OPPIMISKATSAUS

SUOJATTU
TIETOJEN SALAUS
256-bittinen AES-standardi

LAINMUKAINEN
GLOBAALIT STANDARDIT
GDPR- ja CCPA-säädökset

NOLLALUOTTAMUS
KÄYTTÖKÄYTÄNTÖ
Monivaiheinen tunnistautuminen

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: syväverkon ja pimeän verkon väliset erot. Tutustut indeksoimattomiin tietokantoihin, Tor-selaimen sipulireititykseen, .onion-kryptografisiin verkkotunnuksiin ja anonymiteetin tietoturvariskeihin.

TEHTÄVÄMONISTEEN TARKISTUSPISTEET

- [ ] **Osat 1–4: Hallitse kyberturvallisuus ja uhkien ehkäisy.**
- [ ] **Osat 5–7: Ratkaise ristisanatehtäviä ja sanahakuja.**
- [ ] **Osat 8–9: Ratkaise tapaustutkimuksia ja salakirjoitushaaste.**
- [ ] **Osa 10: Tarkista perus- ja jatkotason UKK-sivut.**
- [ ] **Osa 11: Tutustu 10 mielenkiintoiseen tosielämän faktaan.**
- [ ] **Bonus: Nopeat vastaukset -haaste.**

Avaa VPN.comin kyberturvallisuusopas

URL: https://www.vpn.com/fi/kyberturvallisuus/pimea-web-vs-syva-web/

Oppimispolkusi: syväverkon ja pimeän verkon strategia

- Vertaile deep webiä (indeksoimattomat tietokannat) dark webiin (onion-palvelut).
- Ymmärrä, miten sipulireititys salaa ja välittää verkkoliikennettä.
- Arvioi vahvistamattomien Tor-verkon sivustojen käytön tietoturvariskejä.
- Ota käyttöön suojattu yhdyskäytävä ja hiekkalaatikkokäytännöt uhkatiedon keruuroboteille.
- Analysoi onion-palveludomainien salaustekniikkaan perustuvaa osoitemuotoa.

SYVÄVERKON JA PIMEÄN VERKON OPAS: OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: yksityisyys syvässä verkossa ja pimeässä verkossa. Lopuksi bonustehtävä Nopeat vastaukset.

SYVÄVERKON TIETOKANNAT JA PIMEÄN VERKON SIPULIREITITYS (JOHDANTO)

Syvä verkko koostuu indeksoimattomista sivuista salasanojen ja kirjautumisten takana, kuten yksityisistä sähköposteista tai yritysten pankkiportaaleista. Pimeä verkko on syvän verkon osajoukko, joka on tarkoituksella piilotettu ja johon pääsee anonyymisti vain erikoisselaimilla (kuten Tor) ja onion-verkoilla.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. Mikä erottaa syvän verkon pintaverkosta?

- A. Syväverkon sivuja ei indeksoida julkisissa hakukoneissa
- B. Syvän verkon liikenne on laitonta, ja viranomaiset valvovat sitä
- C. Syvän verkon sivustojen käyttö edellyttää erikoisselaimia, kuten Toria
- D. Deep web -sivut latautuvat aina nopeammin kuin pintaverkon sivut

2. Miten pimeään verkkoon päästään?

- A. Sipulireititysverkkoja käyttävien erikoisselainten kautta
- B. Määrittämällä mukautetut DNS-asetukset tavallisiin reitittimiin
- C. Yksityisten, vain kutsutuille tarkoitettujen pintaverkon hakukonsolien kautta
- D. Asentamalla tavallisen mainoksia estävän selainlaajennuksen

3. Mikä rakenne muodostaa syvän verkon suurimman osan?

- A. Salasanasuojatut käyttäjätietokannat ja yksityiset tilit
- B. Laittomat mustan pörssin foorumit, joilla kaupataan laittomia tuotteita
- C. Salaamattomat vertaisverkkotiedostonjakoprotokollat
- D. Julkisten hakukoneiden välimuistitietokannat

4. Mitä sipulireititys (Onion Routing) tekee verkkoliikenteelle?

- A. Se salaa paketit ja reitittää ne useiden välityssolmujen kautta
- B. Se nopeuttaa latauksia ohittamalla internetyhteyden tarjoajan solmut
- C. Se yhdistää laitteiden sarjanumerot IP-tietueisiin
- D. Se poistaa selaimen evästeet jokaisen napsautuksen jälkeen

5. Mitä verkkotunnuksen päätettä käytetään yksinomaan Tor-verkoissa?

- A. Salaustekniikkaan perustuva .onion-ylätason pääte
- B. Tavallinen vanha kaupallinen .com-pääte
- C. Web3-hajautettu .eth-lohkoketjupääte
- D. Maatunnuksen .ai-teknologiapääte

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys tf 6

6. Syvä verkko ja pimeä verkko tarkoittavat samaa verkon osaa.

- ( ) Tosi
- ( ) Epätosi

7 Kysymys tf 7

7. Yritysten intranet-portaalit kuuluvat deep webiin.

- ( ) Tosi
- ( ) Epätosi

8 Kysymys tf 8

8. Sipulireititys purkaa tietopaketit kokonaan jokaisessa läpikulkusolmussa.

- ( ) Tosi
- ( ) Epätosi

9 Kysymys tf 9

9. Pimeän verkon käyttö altistaa laitteet suurille haittaohjelmariskeille.

- ( ) Tosi
- ( ) Epätosi

10 Kysymys tf 10

10. Tavalliset verkkohakukoneet ryömivät ja indeksoivat onion-sivustoja.

- ( ) Tosi
- ( ) Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

Lue jokainen alla oleva lause ja täytä aukko oikealla termillä sanapankista.

1. Yksityiset pankkiportaalit sijaitsevat indeksoimattomassa _____ -osassa.

2. Erikoistuneet Tor-solmut isännöivät piilotettuja palveluja, jotka kuuluvat osaan nimeltä _____ .

3. Tor-sivustot käyttävät kryptografista ylätason päätettä nimeltä _____ .

4. Salattua monikerroksista liikenteen reititystä kutsutaan nimellä _____ .

5. Pintahakukoneet käyvät läpi julkisia sivuja, joita kutsutaan nimellä _____ .

6. Sipuliverkot salaavat asiakkaiden IP-osoitteet; näin säilytetään käyttäjän ominaisuus nimeltä _____ .

SANASTON SANAPANKKI

.ONION ALKUSOLMU ANONYYMIUS INDEKSOIDUT SIVUT PIMEÄ VERKKO SIPULIREITITYS SYVÄ VERKKO TIETOKANTA

Kirjoita vastauksesi tähän:

1. | **2.**

3. | **4.**

5. | **6.**

Tarkistuspiste 4: Tietoturvakäsitteiden yhdistäminen

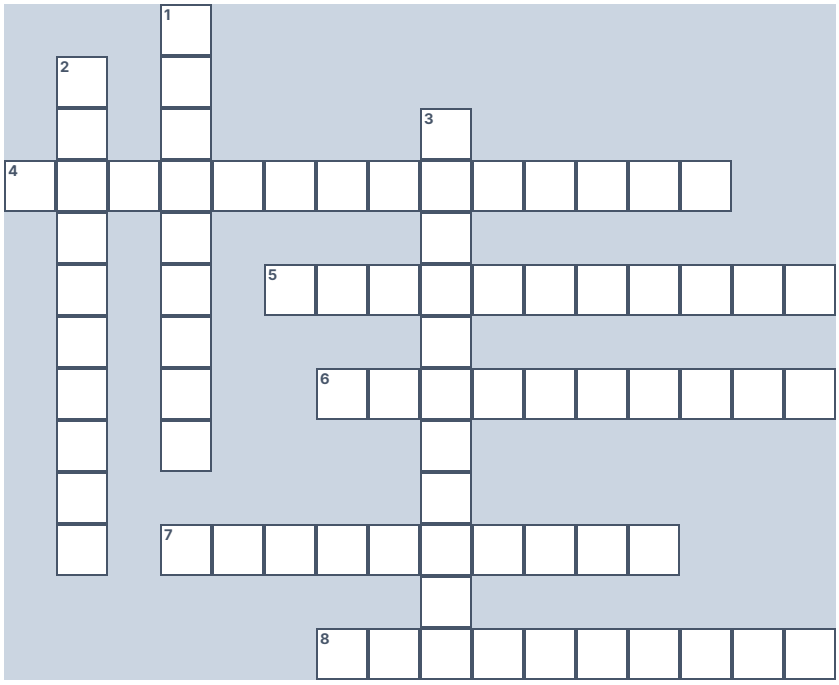
MÄÄRITELMIEN YHDISTÄMINEN

Yhdistä kukin vasemman puolen sanastotermi oikean puolen oikeaan määritelmään kirjoittamalla vastaava kirjain (A–H) täytettävään kenttään.

☐	1. Syväverkon osa	A	Salattu verkon segmentti, johon pääsee vain erityisillä selaimilla.
☐	2. Pimeän verkon portaali	B	Datan salaaminen kerroksittain ja sen välittäminen kolmen solmun kautta.
☐	3. Onion-pääte	C	Suojattu taustatallennustila, jossa säilytetään indeksoimattomia järjestelmätietueita.
☐	4. Tor-reititys	D	Tor-verkoissa käytetty kryptografinen ylätason verkkotunnuspääte.
☐	5. Indeksoidut sivut	E	Sisääntulosolmu, jonka kautta Tor-verkkoon päästään.
☐	6. Käyttäjän anonymiteetti	F	Googlessa koottu ja haettavissa oleva pintaverkon sisältö.
☐	7. Yksityinen tietokanta	G	Asiakkaiden julkisten IP-osoitteiden pitäminen piilossa palvelimilta.
☐	8. Sisääntuloyhdyskäytävä	H	Indeksoimaton verkkosisältö, kuten yksityiset kirjautumiset, sähköpostit ja tietokantatietueet.

Tarkistuspiste 5: Ristikko

Ratkaise ristikko kirjoittamalla kirjaimia aktiivisiin valkoisiin ruutuihin. Numerot vastaavat alla olevia vihjeitä.



VAAKASUORAAN

4. Datan salaaminen kerroksittain ja välittäminen kolmen solmun kautta (14)

5. Pintaverkon sisältö, joka on koottu ja haettavissa Googlessa (11)

6. Indeksoimaton verkkosisältö, kuten yksityiset kirjautumiset, sähköpostit ja tietokantamerkinnät (10)

7. Suojattu taustatallennus, joka isännöi indeksoimattomia järjestelmätietoja (10)

8. Asiakkaiden julkisten IP-osoitteiden pitäminen piilossa palvelimilta (10)

PYSTYSUORAAN

1. Sisääntulosolmu, jonka kautta Tor-verkkoon päästään (9)

2. Kryptografinen ylätason verkkotunnuspääte, jota käytetään Tor-verkoissa (10)

3. Salattu verkon osa, johon pääsee vain erityisten selainten kautta (11)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

Näytönlukijan ja näppäimistön käyttäjät voivat kirjoittaa ristikon vastaukset suoraan alla oleviin tekstikenttiin.

VAAKASUORAAN

4 vaakasuoraan: Datan salaaminen kerroksittain ja välittäminen kolmen solmun kautta (14 kirjainta):

5 vaakasuoraan: Pintaverkon sisältö, joka on koottu ja haettavissa Googlessa (11 kirjainta):

6 vaakasuoraan: Indeksoimaton verkkosisältö, kuten yksityiset kirjautumiset, sähköpostit ja tietokantamerkinnät (10 kirjainta):

7 vaakasuoraan: Suojattu taustatallennus, joka isännöi indeksoimattomia järjestelmätietoja (10 kirjainta):

8 vaakasuoraan: Asiakkaiden julkisten IP-osoitteiden pitäminen piilossa palvelimilta (10 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Sisääntulosolmu, jonka kautta Tor-verkkoon päästään (9 kirjainta):

2 pystysuoraan: Kryptografinen ylätason verkkotunnuspääte, jota käytetään Tor-verkoissa (10 kirjainta):

3 pystysuoraan: Salattu verkon osa, johon pääsee vain erityisten selainten kautta (11 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

Etsi ruudukosta 8 piilotettua keskeistä sanastotermiä. Sanat voivat olla vaaka-, pysty- tai vinosuunnassa.

I N D E K S O I D U T C N Ö Ä
O G S U I M Y Y N O N A Å Q Y
K X M X R B P Y V N H X D Ä X
K L T B Z Ö Å N T S Å J Q E A
R O K K R E V Ä V Y S D L S Y
E Z Z M K I W I G B F J L V U
V Y T Ö F I F U C A M R C Ö N
Ä L Y T W U M L O S U K L A A
E U Z K N N H I O I T G M V M
M T A T N A K O T E I T Z I B
I S I P U L I R E I T I T Y S
P W G Ä P Ä Z U I V Å A R X P
P Ö O N I O N P Ä Ä T E Q J R
V I R X W Q W W L A F Q O M B
P X G H R S Z Ä K L X K Ä Y Å

SANASTOLISTA

SYVÄVERKKO
PIMEÄVERKKO
ONIONPÄÄTE
SIPULIREITITYS
INDEKSOIDUT
ANONYYMIUS
TIETOKANTA
ALKUSOLMU

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

Yhdistä kukin sanahaun 8 sanastotermistä sen oikeaan määritelmään kirjoittamalla kirjain (A–H) tyhjään kohtaan.

SANASTOTERMIT

- **A. SYVÄVERKKO**
- **B. PIMEÄVERKKO**
- **C. ONIONPÄÄTE**
- **D. SIPULIREITITYS**
- **E. INDEKSOIDUT**
- **F. ANONYYMIUS**
- **G. TIETOKANTA**
- **H. ALKUSOLMU**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Asiakkaiden julkisten IP-osoitteiden pitäminen piilossa palvelimilta.
2. Suojattu taustatallennus, joka isännöi indeksoimattomia järjestelmätietoja.
3. Datan salaaminen kerroksittain ja välittäminen kolmen solmun kautta.
4. Indeksoimaton verkkosisältö, kuten yksityiset kirjautumiset, sähköpostit ja tietokantamerkinnät.
5. Salattu verkon osa, johon pääsee vain erityisten selainten kautta.
6. Kryptografinen ylätason verkkotunnuspääte, jota käytetään Tor-verkoissa.
7. Sisääntulosolmu, jonka kautta Tor-verkkoon päästään.
8. Pintaverkon sisältö, joka on koottu ja haettavissa Googlessa.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

Selvitä alla olevat kirjaimet paljastaaksesi keskeisiä kyberturvallisuuden käsitteitä ja termejä. Kirjoita vastauksesi annettuihin syöttökenttiin.

1. K R E V Y S K O Ä V
2. T O O N N E Ä Ä P I
3. I O S I D N U T K D E
4. K T O A T N A T I E
5. K I R E M O Ä V P K E
6. I R I L P T E Y T S I I S U
7. N N A M Y I U S Y O
8. U S M A U L O L K

Bonustehtävä: Nopeat vastaukset

3 VASTAUSTA JOKAISEEN LUOKKAAN. VOITTAJA ON SE, JOKA TÄYTTÄÄ LISTAN ENSIMMÄISENÄ.

1	Syitä pysyä erossa pimeästä verkosta			
2	Asioita, joita hakukone ei löydä			
3	Laitteita, jotka voidaan hakkeroida			
4	Laillisia syitä käyttää Toria			
5	Syitä päivittää ohjelmistot			
6	Varoitusmerkkejä sähköpostissa			
7	Asioita, joita myydään laittomasti pimeässä verkossa			
8	Ihmisiä, joilta voit pyytää IT-apua			
9	Turvallisia tapoja, joita voit aloittaa tänään			
10	Asioita, joita teet tietovuodon jälkeen			
11	Asioita, jotka kuuluvat syvään verkkoon			
12	Sivustoja, joita käytät kirjautumalla			
13	Anonymiteettiin liittyviä sanoja			
14	Tietoja, joita sinun ei pitäisi koskaan jakaa			
15	Asioita, jotka ovat "pinnan alla"			

Tarkistuspiste 8: Kyberturvallisuuden tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: TIETOVUODON TUNNISTAMINEN

👷

Tilanne: Yrityksen tietoturvatarkastus paljastaa, että arkaluonteisia asiakastietokannan tietueita kaupataan onion-markkinapaikalla. Tietoja ei ole indeksoitu Googlessa.

Keskustelukysymys: Selitä, mitkä verkon osat ovat mukana ja miten tämä vuoto tapahtui.

TAPAUSTUTKIMUS 2: ANONYYMIYS VS. HAITTAOHJELMARISKIT

👷

Tilanne: Analyytikko haluaa tarkistaa uhkatiedustelusyötteitä Tor-verkkosivustolta. Hän lataa Tor-selaimen ja avaa sivuston.

Keskustelukysymys: Arvioi anonymiteetin edut ja kuvaa haittaohjelmien torjuntavaiheet.

Tarkistuspiste 9: Salakirjoituksen purkaminen

Kyberturvallisuuden ammattilainen suojaa verkon resursseja verkkohyökkääjiltä. Käytä alla olevaa kirjain–numero-avainta purkaaksesi viestin kirjoittamalla vastaavat kirjaimet tyhjiin kohtiin.

KIRJAIN-NUMERO-SALAUSAVAIN

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26 Å=27 Ä=28 Ö=29

19	28	9	12	25	20	28		11	28	25	20	20	28	10	28	14			
							1	14	15	14	25	25	13	9	21	19			
19	9	16	21	12	9	18	5	9	20	9	20	25	11	19	5	12	12	28	

Purettu viesti:

VIHJE: JOKAINEN NUMERO VASTAA KIRJAIMEN PAIKKAA AAKKOSISSA (ESIM. 1 = A, 2 = B, 29 = Ö).

Tarkistuspiste 10: Usein kysytyt kysymykset kyberturvallisuudesta, perustaso (Osa A)

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q1: Mikä on syvä verkko?

Syvä verkko koostuu kaikista verkkosivuista, joita hakukoneet eivät voi indeksoida, kuten verkkopankista, sähköpostitietokannoista ja maksumuurin takana olevista lehdistä.

Q2: Mikä on pimeä verkko?

Pimeä verkko on syvän verkon pieni, tarkoituksella piilotettu osa, johon pääsee vain onion-verkkoja käyttävillä erikoisselaimilla.

Q3: Miten hakukoneet indeksoivat sivuja?

Hakukoneet ajavat automaattisia ohjelmia (hakurobotteja) seuraamaan julkisia linkkejä ja indeksoivat sivut, joita ei ole estetty indeksoinnilta robot-direktiiveillä.

Q4: Miksi verkkopankkia pidetään osana syvää verkkoa?

Pankkiportaalit ovat kirjautumisseinien ja salasanojen takana, mikä estää julkisia hakukoneita indeksoimasta tiliotesivuja.

Q5: Mitä Tor-selaimen sipulireititys on?

Sipulireititys on siirtotapa, joka salaa liikenteen kerroksittain ja välittää sen usean releen kautta käyttäjien IP-osoitteiden peittämiseksi.

Tarkistuspiste 10: Usein kysytyt kysymykset kyberturvallisuudesta, perustaso (Osa B)

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q6: Onko pimeään verkkoon pääsy laitonta?

Ei. Pimeän verkon käyttö on laillista useimmissa maissa, mutta laittomilla markkinapaikoilla toimiminen tai kyberrikollinen toiminta on kiellettyä.

Q7: Miksi pimeän verkon sivustot latautuvat hitaasti?

Liikenne reititetään ja salaus puretaan vähintään kolmen maailmanlaajuisen välityssolmun (sisääntulo, väli, poistuminen) kautta, mikä pidentää siirtoviivettä.

Q8: Mitä .onion-verkkotunnuspääte tarkoittaa?

Se on Tor-verkoissa käytettävä erikoistunut ylätason verkkotunnuspääte, joka osoittaa kryptografisesti luotuihin osoitteisiin tavallisten DNS-palvelimien sijaan.

Q9: Mitä riskejä pimeän verkon linkkeihin liittyy?

Sivustoilla ei ole tietoturvaseulontaa, mikä altistaa käyttäjät korkeille haittaohjelmatartuntojen, tietojenkalastelukomentosarjojen ja tapahtumahuijausten määrille.

Q10: Kuka loi Tor-verkon reititysprotokollan?

Teknologian kehitti alun perin Yhdysvaltain laivaston tutkimuslaboratorio 1990-luvulla hallituksen viestinnän suojaamiseksi.

Tarkistuspiste 10: Usein kysytyt kysymykset tietoturvasta, jatkotaso (Osa C)

Tutustu tietoturvaviitekehysten, haittaohjelma-analyysin ja tietojen vaatimustenmukaisuuden edistyneisiin teknisiin puoliin.

Q1: Miten välisolmut suojaavat Torin anonymiteettiä?

Jokainen solmu purkaa vain yhden kerroksen reititystietoja ja tietää vain edellisen ja seuraavan hypyn, ei koskaan sekä lähdettä että kohdetta.

Q2: Mikä on poistumissolmun tehtävä?

Poistumissolmu purkaa viimeisen salauskerroksen ja lähettää liikenteen julkiselle kohdepalvelimelle tai onion-palvelimelle.

Q3: Mikä on Tor-siltayhdyskäytävä?

Sillat ovat listaamattomia Tor-sisäänkäyntireleitä, joilla ohitetaan internetyhteyden tarjoajan estot ja sensuuri alueilla, jotka rajoittavat Tor-selaimen käyttöä.

Q4: Miten pimeän verkon toimijat hyödyntävät kryptovaluuttoja?

Toimijat käyttävät anonyymejä kryptovaluuttoja talouskauppojen tekemiseen pimeillä markkinapaikoilla ja kiertävät tavanomaiset pankkitapahtumien tarkistukset.

Q5: Miksi tavalliset hakukoneet eivät indeksoi syviä tietokantoja?

Indeksointirobotit eivät voi syöttää kirjautumistietoja, ratkaista tietoturva-CAPTCHAja tai ajaa taustajärjestelmän SQL-kyselykomentosarjoja, joita deep web -tietokantoihin pääsy vaatii.

Tarkistuspiste 10: Usein kysytyt kysymykset tietoturvasta, jatkotaso (Osa D)

Tutustu tietoturvaviitekehysten, haittaohjelma-analyysin ja tietojen vaatimustenmukaisuuden edistyneisiin teknisiin puoliin.

Q6: Mikä on hakemistopalvelin Tor-verkoissa?

Se on luotettu palvelin, joka ylläpitää luetteloa aktiivisista sisäänmeno-, väli- ja poistumisreleistä, joita asiakkaat käyttävät reittien muodostamiseen.

Q7: Miten haitalliset toimijat nuuskivat poistumissolmuja?

Rogue-ulostulosolmujen ylläpitäjät voivat siepata salaamatonta HTTP-liikennettä sen poistuessa Tor-verkosta ja varastaa käyttäjätunnuksia ja evästeitä.

Q8: Mikä on Torin ja I2P:n ero?

Tor käyttää keskitettyä välityssolmuhakemistoa ja poistumissolmuja julkiseen verkkoon pääsyyn, kun taas I2P käyttää hajautettua vertaisverkkorakennetta sisäiseen isännöintiin.

Q9: Miten lainvalvontaviranomaiset seuraavat pimeän verkon markkinapaikkoja?

Viranomaiset käyttävät lohkoketjuanalyysia, paikantavat fyysiset palvelinisännöintijärjestelyt ja suorittavat houkutusoperaatioita ylläpitäjien tunnistamiseksi.

Q10: Miten DNS-vuoto vaarantaa asiakkaan anonymiteetin?

DNS-vuotoja syntyy, kun selaimen DNS-kyselyt lähetetään suoraan paikallisen internetpalveluntarjoajan kautta sen sijaan, että ne reititettäisiin salatun Tor-verkon kautta.

Osa 11: 10 tosielämän kyberturvallisuusfaktaa ja havaintoa

Tutustu todellisiin tosiasioihin tietoturvaloukkauksista, puolustusmekanismeista ja vaatimustenmukaisuusstandardeista.

1. TURVALLISUUSOIVALLUS

Syvä verkko on paljon suurempi kuin haettavissa oleva pintaverkko, sillä suurin osa sisällöstä on kirjautumisten ja tietokantojen takana.

2. TURVALLISUUSOIVALLUS

Pimeä verkko on syvän verkon pieni, tarkoituksella piilotettu osa, johon päästään esimerkiksi Torilla.

3. TURVALLISUUSOIVALLUS

Torin reititys salaa datapaketit kolme kertaa ja kuorii salauskerrokset kuin sipulin jokaisessa välityssolmussa.

4. TURVALLISUUSOIVALLUS

Tor kehittyi Yhdysvaltain laivaston tutkimuslaboratorion johtamasta sipulireititysprojektista, ja sen koodi julkaistiin vapaana ohjelmistona. [1]

5. TURVALLISUUSOIVALLUS

Onion-osoitteet ovat 56 merkin pituisia aakkosnumeerisia merkkijonoja, jotka luodaan kryptografisesti julkisista avainpareista.

6. TURVALLISUUSOIVALLUS

Poistumissolmut voivat lukea selkotekstiliikennettä, joten TLS/HTTPS on edelleen tarpeen Torissa suojattua istuntodataa varten.

7. TIETOTURVATIETOA

Intranet-sivustot, pilvilevyt ja yksityiset tietokannat muodostavat syväverkon suurimmat tietovarastosegmentit.

8. TIETOTURVATIETOA

Erikoishakukoneet, kuten DuckDuckGo, ylläpitävät sipuliportaaleja, jotka mahdollistavat anonyymit haut Tor-verkoissa.

9. TIETOTURVATIETOA

Yli 2 miljoonaa käyttäjää yhdistää Tor-verkkoon päivittäin ohittaakseen sensuurin ja säilyttääkseen viestinnän yksityisyyden.

10. TURVALLISUUSOIVALLUS

Kansainväliset lainvalvontaoperaatiot (kuten Operation Bayonet) sulkivat merkittäviä pimeitä markkinapaikkoja takavarikoimalla palvelinlaitteistoa.

Tekniset viitteet ja lähteet

Opiskeluopas ja interaktiiviset pulmat on koottu maailmanlaajuisista NIST-, OWASP- ja tietosuojavaatimustenmukaisuusstandardeista.

TIETEELLISET JA ALAN VIITTEET

[1] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 **Hakuindeksointi** SYVÄVERKKO Oikea vastaus: A

OPETTAJALLE

Syväverkon sivut ovat kirjautumisseinien ja tietokantojen takana, mikä estää hakurobotteja indeksoimasta niitä. Lähde: IETF RFC 3986.

2 **Torin käyttö** DARK WEB Oikea vastaus: A

OPETTAJALLE

Pimeä verkko koostuu piilotetuista onion-palveluista, joihin pääsee vain Tor-kaltaisilla selaimilla. Lähde: IETF RFC 3986.

3 **Syvät tietokannat** TIETOKANNAT Oikea vastaus: A

OPETTAJALLE

Salasanalla suojatut tilit ja yritysten tiedot muodostavat syvän verkon suurimman osan. Lähde: NIST Digital Identity.

4 **Sipulireititys** TOR-VERKKO Oikea vastaus: A

OPETTAJALLE

Sipulireititys salaa tietopaketit kerroksittain ja välittää ne usean solmun kautta anonymiteetin takaamiseksi. Lähde: IETF RFC 3986.

5 **Onion-verkkotunnus** PÄÄTE Oikea vastaus: A

OPETTAJALLE

Kryptografinen.onion-verkkotunnuspääte reitittää liikenteen Torin sisällä ilman julkista DNS:ää. Lähde: IETF RFC 3986.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Verkkosegmentit** RAKENNE — **Oikea vastaus: Epätosi**

OPETTAJALLE

Syvä verkko kattaa kaikki indeksoimattomat sivut, kun taas pimeä verkko on pieni, salattu onion-osajoukko. Lähde: IETF RFC 3986.

7 **Yritysten intranetit** SYVÄVERKKO — **Oikea vastaus: Tosi**

OPETTAJALLE

Intranet-sivustot ovat salasanaportaalien takana eikä niitä indeksoida, mikä tarkoittaa, että ne kuuluvat syväverkkoon. Lähde: NIST Digital Identity.

8 **Kerrossalaus** VÄLITYSSOLMUT — **Oikea vastaus: Epätosi**

OPETTAJALLE

Onion-releet purkavat vain yhden reitityskerroksen käyttäjän anonymiteetin suojaamiseksi, eivät koskaan koko pakettia. Lähde: IETF RFC 3986.

9 **Haittaohjelmille altistuminen** UHKAT — **Oikea vastaus: Tosi**

OPETTAJALLE

Pimeän verkon kauppapaikoilla ei ole turvallisuussuodatusta, joten haittaohjelmatartuntojen riski on erittäin suuri. Lähde: Center for Internet Security (CIS).

10 **Kysymys 10** — **Oikea vastaus: Epätosi**

OPETTAJALLE

Tavalliset hakukoneiden indeksointirobotit eivät käytä Toria, joten ne eivät pääse .onion-sivustoille eivätkä voi indeksoida niitä.

Sanastoavaimet ja arviointikriteerit

Opettajan arviointikriteeri: Anna 1 piste jokaisesta oikeasta yhdistämisestä (yhteensä 8 pistettä) ja asiayhteystermistä (yhteensä 6 pistettä).

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

H 1. Syväverkon osa	A 2. Pimeän verkon portaali	D 3. Onion-pääte	B 4. Tor-reititys
F 5. Indeksoidut sivut	G 6. Käyttäjän anonymiteetti	C 7. Yksityinen tietokanta	E 8. Sisääntuloyhdyskäytävä

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 SYVÄ VERKKO	2 PIMEÄ VERKKO	3 .ONION	4 SIPULIREITITYS
5 INDEKSOIDUT SIVUT	6 ANONYYMIUS		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 F – ANONYYMIUS	2 G – TIETOKANTA	3 D – SIPULIREITITYS	4 A – SYVÄVERKKO
5 B – PIMEÄVERKKO	6 C – ONIONPÄÄTE	7 H – ALKUSOLMU	8 E – INDEKSOIDUT

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit Syväverkon osa, Pimeän verkon portaali ja Onion-pääte omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

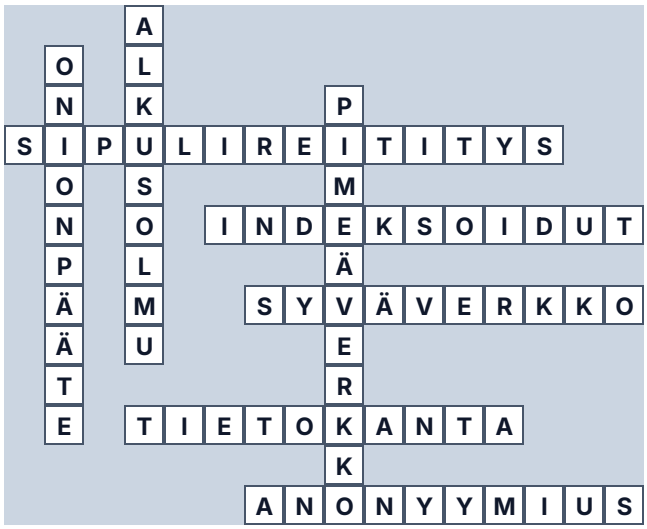
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

I	N	D	E	K	S	O	I	D	U	T	C	N	Ö	Ä
O	G	S	U	I	M	Y	Y	N	O	N	A	Å	Q	Y
K	X	M	X	R	B	P	Y	V	N	H	X	D	Ä	X
K	L	T	B	Z	Ö	Å	N	T	S	Å	J	Q	E	A
R	O	K	K	R	E	V	Ä	V	Y	S	D	L	S	Y
E	Z	Z	M	K	I	W	I	G	B	F	J	L	V	U
V	Y	T	Ö	F	I	F	U	C	A	M	R	C	Ö	N
Ä	L	Y	T	W	U	M	L	O	S	U	K	L	A	A
E	U	Z	K	N	N	H	I	O	I	T	G	M	V	M
M	T	A	T	N	A	K	O	T	E	I	T	Z	I	B
I	S	I	P	U	L	I	R	E	I	T	I	T	Y	S
P	W	G	Ä	P	Ä	Z	U	I	V	Å	A	R	X	P
P	Ö	O	N	I	O	N	P	Ä	Ä	T	E	Q	J	R
V	I	R	X	W	Q	W	W	L	A	F	Q	O	M	B
P	X	G	H	R	S	Z	Ä	K	L	X	K	Ä	Y	Å

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

4 vaakasuoraan: SIPULIREITITYS Datan salaaminen kerroksittain ja välittäminen kolmen solmun kautta (14 kirjainta)

5 vaakasuoraan: INDEKSOIDUT Pintaverkon sisältö, joka on koottu ja haettavissa Googlessa (11 kirjainta)

6 vaakasuoraan: SYVÄVERKKO Indeksoimaton verkkosisältö, kuten yksityiset kirjautumiset, sähköpostit ja tietokantamerkinnät (10 kirjainta)

7 vaakasuoraan: TIETOKANTA Suojattu taustatallennus, joka isännöi indeksoimattomia järjestelmätietoja (10 kirjainta)

8 vaakasuoraan: ANONYYMIUS Asiakkaiden julkisten IP-osoitteiden pitäminen piilossa palvelimilta (10 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: ALKUSOLMU Sisääntulosolmu, jonka kautta Tor-verkkoon päästään (9 kirjainta)

2 pystysuoraan: ONIONPÄÄTE Kryptografinen ylätason verkkotunnuspääte, jota käytetään Tor-verkoissa (10 kirjainta)

3 pystysuoraan: PIMEÄVERKKO Salattu verkon osa, johon pääsee vain erityisten selainten kautta (11 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. KREVYSKOÄV — **SYVÄVERKKO**
2. TOONNEÄÄPI — **ONIONPÄÄTE**
3. IOSIDNUTKDE — **INDEKSOIDUT**
4. KTOATNATIE — **TIETOKANTA**
5. KIREMOÄVPKE — **PIMEÄVERKKO**
6. IRILPTEYTSIISU — **SIPULIREITITYS**
7. NNAMYIUSYO — **ANONYYMIUS**
8. USMAULOLK — **ALKUSOLMU**

SALAKIRJOITUSHAASTEEN AVAIN

"SÄILYTÄ KÄYTTÄJÄN ANONYYMIUS SIPULIREITITYKSELLÄ"

Tapaustutkimusten vastausavain

A Tapaustutkimus 1: Tietovuodon tunnistaminen

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Yrityksen tietoturva-auditointi paljastaa, että arkaluonteisia asiakastietokannan tietueita kaupataan onion-markkinapaikalla. Dataa ei ole indeksoitu Googleen.
- Suositeltu strategia ja ratkaisu: Osallisena olevat segmentit: Yksityinen tietokanta kuuluu syvään verkkoon (indeksoimaton mutta suojattu). Varastettua dataa kauppaava markkinapaikka sijaitsee pimeässä verkossa (onion-verkko). Miten se tapahtui: Hakkerit ohittivat palvelimen suojaukset, varastivat tietokannan syvästä verkosta ja listasivat sen anonyymisti pimeään verkkoon välttääkseen lainvalvonnan jäljityksen.

B Tapaustutkimus 2: Anonyymiys vs. haittaohjelmariskit

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Analyytikko haluaa tarkistaa uhkatietosyötteitä Tor-sivustolla. Hän lataa Tor-selaimen ja avaa sivuston.
- Suositeltu strategia ja ratkaisu: Hyödyt: Tor reitittää liikenteen kolmen solmun kautta ja peittää analyytikon yrityksen IP-osoitteen. Riskit ja lieventäminen: Pimeän verkon linkeillä ei ole maineen seulontaa. Analyytikoiden on ajettava Toria eristetyissä virtuaalikoneissa (VM), poistettava JavaScript käytöstä Torin asetuksissa ja vältettävä tiedostojen lataamista yritysverkon suojaamiseksi.