Nimi: _____ Päivämäärä: _____ Pisteet: _____

Julkisen Wi-Fin turvallisuus ja salaus

Mies välissä -hyökkäykset, vilpilliset tukiasemat, pakettien nuuskinta, VPN-tunnelit ja HTTPS-salaus.

JULKISEN WI-FIN TURVALLISUUS, OPPIMISKATSAUS

SUOJATTU
TIETOJEN SALAUS
256-bittinen AES-standardi

LAINMUKAINEN
GLOBAALIT STANDARDIT
GDPR- ja CCPA-säädökset

NOLLALUOTTAMUS
KÄYTTÖKÄYTÄNTÖ
Monivaiheinen tunnistautuminen

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: julkisen Wi-Fin turvallisuus. Tutustut salaamattomiin verkkoihin, välimieshyökkäyksiin (MitM), kaappaustukiasemiin, pakettien nuuskintaan, VPN-tunneleihin ja HTTPS-siirron turvallisuuteen.

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/julkisen-wifin-tietoturva/

Oppimispolkusi: julkisen Wi-Fin turvallisuus

- Tunnista julkisten Wi-Fi-verkkojen yleiset riskit, kuten pakettien nuuskinta ja luvattomat tukiasemat.
- Toteuta VPN-salaustunnelit siirrettävien tietojen suojaamiseksi.
- Pakota HTTPS ja turvalliset selainasetukset etätyöntekijöille.

JULKISEN WI-FIN TURVAOPAS, OHJEET

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

JULKISEN WI-FIN TURVALLISUUS JA SIIRRON SUOJAUS (JOHDANTO)

Salaamattomat julkiset Wi-Fi-hotspotit jättävät verkkoliikenteen alttiiksi pakettien nuuskimiselle ja Evil Twin -huijauksille. Liikenteen pakottaminen suojattujen VPN-salaustunnelien kautta ja vain HTTPS:ää koskevien HSTS-sääntöjen noudattaminen suojaa istuntoja paikallisverkon sieppaukselta.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. Mikä on välimieshyökkäys (Man-in-the-Middle, MitM)?

- A. Kahden osapuolen välisen viestinnän sieppaaminen ja muuttaminen jaetussa verkossa
- B. Tietokannan poimintatekniikka, joka kohdistuu käyttäjätietueisiin
- C. Verkkopalvelinten ylikuormittaminen verkkoliikennepyynnöillä
- D. Paikallisten kiintolevytallennusmedioiden tyhjentäminen

2. Mikä on kaappaustukiasema (Evil Twin)?

- A. Haitallinen Wi-Fi-hotspot, joka on määritetty samalla SSID:llä kuin oikea verkko
- B. Hallintatyökalu, jolla valvotaan tietokantojen varmuuskopioita
- C. Suojattu VPN-yhdyskäytävän määritys
- D. DNS-tietue, joka kartoittaa valtuutetut postipalvelimet

3. Miten VPN suojaa julkisen Wi-Fi-verkon liikennettä?

- A. Se käärii kaikki verkkopaketit salattuun tunneliin, jolloin nuuskijat eivät pysty lukemaan niitä
- B. Se estää automaattisesti kaikki saapuvat yhteyspyynnöt
- C. Se muuttaa fyysisen verkkokortin MAC-osoitetta
- D. Se poistaa selaimen välimuistissa olevat evästeet

4. Mitä on pakettien nuuskinta (packet sniffing)?

- A. Laitteisto- tai ohjelmistotyökalujen käyttö verkkopakettien sieppaamiseen ja kirjaamiseen
- B. Paikallisten hakemistojen skannaus kaksoiskappaleiden löytämiseksi
- C. Tietokannan lukuoikeuksien rajoittaminen käyttäjärooleihin perustuen
- D. Tallennusasemien salaus AES-256-avaimilla

5. Mikä on HTTPS:n tehtävä?

- A. Selaimen ja verkkopalvelimen välisen istuntoliikenteen salaus
- B. Saapuvien sähköpostiviestien suodattaminen yhdyskäytävässä
- C. Kuvien pakkaaminen nopeampaa sivunlatausta varten
- D. Tiedostorakenteiden hallinta verkkoon liitetyssä tallennustilassa

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Yhdistyneet käyttäjät voivat helposti kaapata selväkielistä dataa avoimissa julkisissa Wi-Fi-verkoissa.

- ○ Tosi
- ○ Epätosi

7 Kysymys 7

7. Väärennetyt tukiasemat (Evil Twin) ovat aina verkon ylläpitäjien valtuuttamia.

- ○ Tosi
- ○ Epätosi

8 Kysymys 8

8. VPN ei suojaa tehokkaasti liikennettä pakettien nuuskimiselta julkisissa verkoissa.

- ○ Tosi
- ○ Epätosi

9 Kysymys 9

9. HTTPS salaa vain URL-polun ja jättää pakettien hyötykuorman selkotekstiksi.

- ○ Tosi
- ○ Epätosi

10 Kysymys 10

10. WPA3-suojausta käyttävät Wi-Fi-hotspotit tarjoavat vahvemman suojan kuin avoimet, salasanattomat verkot.

- ○ Tosi
- ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Yksityisten salasanojen kaappaaminen julkisessa Wi-Fi-verkossa on viestinnän _____ .
2. Raakapakettien analysointi paikallisverkossa tehdään pakettien _____ .
3. Hotellin Wi-Fi-verkkoa jäljittelevä väärä hotspot on _____ .
4. Verkkoliikenteen siirron suojaaminen edellyttää salausta protokollalla _____ .
5. Kaikki verkkolähdöt salaava asiakasohjelma on _____ .
6. Salattu viestintäreitti julkisten verkkojen läpi on _____ .

SANASTON SANAPANKKI

EVIL TWIN HTTPS KAAPPAUS PALOMUURI SNIFFAUS TUNNELI VPN WPA-SUOJAUS

Kirjoita vastauksesi tähän:

1.
2.
3.
4.
5.
6.

Tarkistuspiste 4: Tietoturvakäsitteiden yhdistäminen

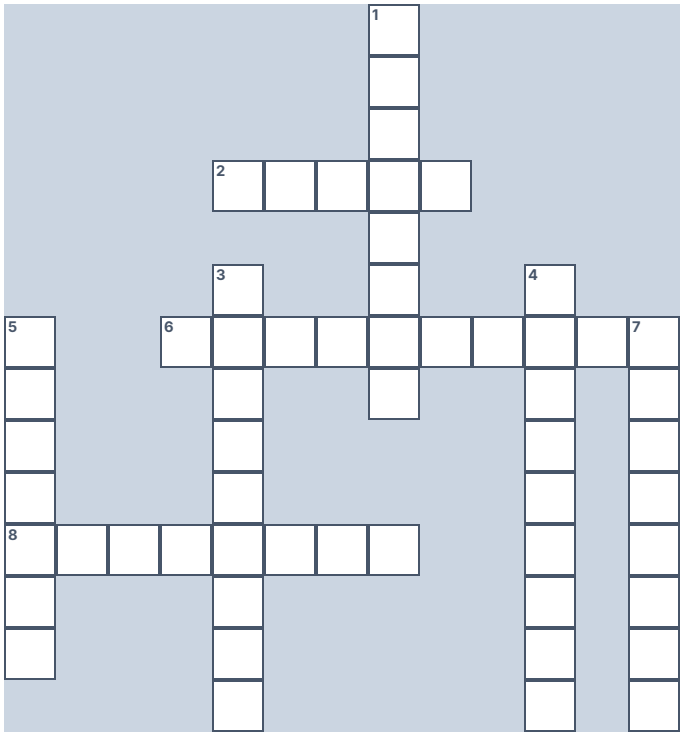
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. SALAKUUNTELU	A	Moderni Wi-Fi-tietoturvastandardi.
☐	2. NUUSKINTA	B	Suojattu datareitti siirron aikana.
☐	3. EVIL TWIN	C	Saapuvan liikenteen suodatus.
☐	4. HTTPS	D	Wi-Fi-verkkoa jäljittelevä väärennetty hotspot.
☐	5. VPN	E	Liikenteen lukeminen siirron aikana.
☐	6. TUNNELI	F	Verkon datapakettien kaappaaminen.
☐	7. WPA3	G	Salattu virtuaalinen yksityisverkko.
☐	8. PALOMUURI	H	Suojattu verkkoyhteys.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

2. Suojattu verkkoliikenne. (5)

6. Moderni Wi-Fi-suojausstandardi. (10)

8. Wi-Fi-verkkoa jäljittelevä väärä hotspot. (8)

PYSTYSUORAAN

1. Liikenteen lukeminen siirron aikana. (8)

3. Salattu virtuaalinen yksityisverkko. (9)

4. Saapuvan liikenteen suodatus. (9)

5. Suojattu datareitti siirron aikana. (7)

7. Verkon datapakettien kaappaaminen. (8)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

2 vaakasuoraan: Suojattu verkkoliikenne. (5 kirjainta):

6 vaakasuoraan: Moderni Wi-Fi-suojausstandardi. (10 kirjainta):

8 vaakasuoraan: Wi-Fi-verkkoa jäljittelevä väärä hotspot. (8 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Liikenteen lukeminen siirron aikana. (8 kirjainta):

3 pystysuoraan: Salattu virtuaalinen yksityisverkko. (9 kirjainta):

4 pystysuoraan: Saapuvan liikenteen suodatus. (9 kirjainta):

5 pystysuoraan: Suojattu datareitti siirron aikana. (7 kirjainta):

7 pystysuoraan: Verkon datapakettien kaappaaminen. (8 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

KAAPPAUS SNIFFAUS EVILTWIN HTTPS VPNYHTEYS TUNNELI
WPASUOJAUS PALOMUURI

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. KAAPPAUS**
- **B. SNIFFAUS**
- **C. EVILTWIN**
- **D. HTTPS**
- **E. VPNYHTEYS**
- **F. TUNNELI**
- **G. WPASUOJAUS**
- **H. PALOMUURI**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Moderni Wi-Fi-suojausstandardi.
2. Wi-Fi-verkkoa jäljittelevä väärä hotspot.
3. Verkon datapakettien kaappaaminen.
4. Suojattu datareitti siirron aikana.
5. Saapuvan liikenteen suodatus.
6. Liikenteen lukeminen siirron aikana.
7. Salattu virtuaalinen yksityisverkko.
8. Suojattu verkkoliikenne.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. **UPPKAASA** _____
2. **LENVIWTI** _____
3. **VTHPESYYN** _____
4. **OUUSSAJWPA** _____
5. **FANSFSUI** _____
6. **PHTST** _____
7. **TLEIUNN** _____
8. **IMRPOAUUL** _____

Bonustehtävä: Nopeat vastaukset

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

1	Syitä päivittää ohjelmistot			
2	Laitteita, jotka yhdistyvät Wi-Fiin automaattisesti			
3	Tietoja, joita sinun ei pitäisi koskaan jakaa			
4	Turvallisia tapoja, joita voit aloittaa tänään			
5	Tapoja pysyä turvassa kahvilassa			
6	Laitteita, jotka voidaan hakkeroida			
7	Asioita, jotka hakkeri voi nähdä avoimessa Wi-Fissä			
8	Merkkejä väärennetystä Wi-Fi-verkosta			
9	Vaihtoehtoja julkiselle Wi-Fille			
10	Varoitusmerkkejä sähköpostissa			
11	Asioita, joita et tee julkisessa Wi-Fissä			
12	Paikkoja, joissa on ilmainen Wi-Fi			
13	Tapoja suojata tilisi			
14	Merkkejä siitä, että tietokone on saanut tartunnan			
15	Wi-Fi-nimiä, jotka vaikuttavat epäilyttäviltä			

Tarkistuspiste 8: Kyberturvallisuuden tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: JULKISEN WI-FI-YHTEYDEN PAKETTINUUSKINNAN ERISTÄMINEN



Tilanne: Julkiseen lentokentän Wi-Fi-verkkoon yhdistetty etämyyntijohtaja huomaa, että useita arkaluonteisia liikesähköposteja vuotaa pian sen jälkeen, kun ne on lähetetty selkokielisinä.

Keskustelukysymys: Analysoi julkisten verkkojen riskit ja kuvaa liikenteen salausratkaisu.

TAPAUSTUTKIMUS 2: EVIL TWIN -VALEHOTSPOTIN TORJUNTA



Tilanne: Hyökkääjät pystyttävät luvattoman langattoman tukiaseman nimeltä "CoffeeShop_Guest", joka jäljittelee oikeaa kahvilan hotspotia ja kaappaa verkkoliikennettä epäilemättömiltä vierailta.

Keskustelukysymys: Kuvaa varmennusvaiheet luvattomien tukiasemien havaitsemiseksi ja estämiseksi.

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	1	12	1	1		10	21	12	11	9	19	5	14		23	9	6	9	14
		12	9	9	11	5	14	14	5		22	16	14		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: Miksi julkinen Wi-Fi on turvaton?

Avoin julkinen Wi-Fi ei salaa liikennettä ilmassa, joten lähellä olevat voivat siepata kaiken suojaamattoman datan. [2]

Q2: Mitä on pakettinuuskinta?

Pakettinuuhkija sieppaa verkkoliittymässä kulkevan raakadatan ja paljastaa selkotekstisalasanat ja liikenteen tiedot.

Q3: Mikä on Evil Twin?

Hakkereiden pystyttämä vilpillinen tukiasema, joka jäljittelee luotetun paikallisen Wi-Fi-hotspotin nimeä ja asetuksia.

Q4: Miten VPN suojaa minua?

Se reitittää liikenteesi salatun tunnelin kautta ja piilottaa selaustoimintasi paikallisverkon nuuskijoilta.

Q5: Suojaako HTTPS minua julkisessa Wi-Fi-verkossa?

Kyllä, se salaa selaimesi ja verkkosivuston välillä vaihdettavat tiedot, ja VPN lisää suojaan vielä yhden kerroksen.

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

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q6: Mikä on WPA3?

Moderni Wi-Fi Protected Access -standardi, joka tarjoaa vahvemman salauksen ja suojan offline-sanakirjahyökkäyksiä vastaan. [1]

Q7: Voiko julkinen Wi-Fi toimittaa haittaohjelmia?

Kyllä, hyökkääjät voivat siepata liikenteen ja syöttää selaimesi istuntoon haitallisia latauskehotteita (drive-by-lataukset).

Q8: Mikä on tiedostonjaon riski?

Jos tiedostojen jako on käytössä, muut julkisen verkon käyttäjät voivat lukea tai muokata paikallista kansiohakemistoasi.

Q9: Mikä on kirjautumisportaali (captive portal)?

Hotellien tai kahviloiden verkkojen kirjautumissivu, jolla annetaan internetyhteys ja jonka hyökkääjät voivat joskus väärentää.

Q10: Pitäisikö minun sammuttaa Wi-Fi, kun en käytä sitä?

Kyllä, Wi-Fin poistaminen käytöstä estää laitettasi muodostamasta automaattisesti yhteyttä epäluotettaviin verkkoihin.

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

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

Q1: Miten välimieshyökkäys (Man-in-the-Middle) hyödyntää DNS:ää?

Käyttämällä DNS-väärennystä vilpillisessä reitittimessä ohjaamaan kohdeselaimet samannäköisille tietojenkalastelusivuille kohdeverkkotunnusten sijaan.

Q2: Mitä on istunnon kaappaus?

Hyökkääjä nuuskii salaamattoman istuntoevästeen julkisessa Wi-Fi-verkossa ja tuo sen käyttöön kirjautumistietojen ohittamiseksi.

Q3: Mitä SSL stripping on?

MitM-hyökkäys, jossa hyökkääjä alentaa käyttäjän suojatun HTTPS-pyynnön salaamattomaksi HTTP:ksi ja kaappaa kirjautumistiedot selkotekstinä.

Q4: Miten HSTS suojaa SSL stripping -hyökkäykseltä?

HTTP Strict Transport Security pakottaa selaimet muodostamaan yhteyden vain HTTPS:n kautta ja kieltäytyy salaamattomista HTTP-varayhteyksistä. [3]

Q5: Mikä on jaetun tunneloinnin VPN?

Määritys, joka reitittää vain yritysliikenteen VPN:n kautta ja lähettää julkisen internetliikenteen suoraan, mikä voi aiheuttaa vuotoreitin paljastumisen riskin.

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

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

Q6: Miksi WPA2 on haavoittuva KRACK-hyökkäykselle?

Key Reinstallation Attack hyödyntää WPA2:n nelivaiheista kättelyä pakettien salauksen purkamiseen ilman Wi-Fi-salasanaa.

Q7: Mitä asiakkaiden eristäminen on?

Reitittimen suojausasetus, joka estää yhdistettyjä Wi-Fi-laitteita viestimästä suoraan keskenään ja estää paikallisen nuuskimisen.

Q8: Miten hyökkääjät käyttävät väärennettyjä DNS-palvelimia?

Ne määrittävät luvattomat reitittimet antamaan asiakkaille väärennettyjä DNS-palvelimia, jolloin ne voivat siepata ja kirjoittaa uudelleen kaikki verkkohaut.

Q9: Voiko VPN piilottaa paikallisen MAC-osoitteeni?

Ei. MAC-osoitteet ovat paikallisia kerros 2 -tunnisteita; käytä sen sijaan laitteesi sisäänrakennettua MAC-satunnaistusta (yksityinen osoite).

Q10: Mikä on captive portal -väärennöshyökkäys?

Hyökkääjä, joka ylläpitää väärennettyä todennusportaalia väärennetyssä hotspotissa varastaakseen tunnistetietoja ilmaisen Wi-Fi-yhteyden varjolla.

Osa 11: 10 tosielämän kyberturvallisuusfaktaa ja havaintoa

Tutustu todellisiin tosiasioihin tietoturvaloukkauksista, puolustusmekanismeista ja vaatimustenmukaisuusstandardeista.

1. TURVALLISUUSOIVALLUS

Etätyöntekijät käyttävät usein kahviloiden, hotellien ja lentokenttien Wi-Fi-verkkoja, joiden turvallisuutta he eivät voi hallita.

2. TURVALLISUUSOIVALLUS

Evil Twin -väärennetty hotspot voi kopioida luotetun verkon täsmällisen nimen ja MAC-osoitteen ja hämätä laitteita.

3. TURVALLISUUSOIVALLUS

Pakettiverkon nuuskintaohjelmistot, kuten Wireshark, ovat ilmaisia ja voivat näyttää salaamattomia HTTP-salasanoja selkotekstinä.

4. TURVALLISUUSOIVALLUS

WPA3-suojaus käyttää Simultaneous Authentication of Equals (SAE) -menetelmää paikallisten raakaa voimaa käyttävien hyökkäysten torjuntaan.

5. TURVALLISUUSOIVALLUS

SSL-strippaushyökkäykset ohittavat HTTPS:n perussuojaukset sieppaamalla alkuperäiset HTTP-uudelleenohjaukset yhdyskäytävässä.

6. TURVALLISUUSOIVALLUS

HTTP Strict Transport Security (HSTS) -vastausotsakkeet estävät selaimia palaamasta salaamattomiin HTTP-yhteyksiin. [3]

7. TIETOTURVATIETOA

Kun 'Auto-Connect' kytketään pois päältä, älypuhelimet eivät yhdisty julkisissa tiloissa oleviin samannäköisiin luvattomiin verkkoihin.

8. TIETOTURVATIETOA

Yritysten "always-on" VPN -määritykset pakottavat kaiken etätyöntekijöiden verkkoliikenteen yrityksen palomuurien läpi.

9. TIETOTURVATIETOA

Väärennetyt tukiasemat voivat jakaa väärennettyjä DNS-vastauksia ja ohjata kohdeverkkotunnukset tietojenkalastelupalvelimille.

10. TURVALLISUUSOIVALLUS

Ilman VPN:ää avoimen hotspotin muut käyttäjät voivat nähdä, mihin sivustoihin ja palvelimiin laitteesi ottaa yhteyttä.

Tekniset viitteet ja lähteet

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

TIETEELLISET JA ALAN VIITTEET

[1] Wi-Fi Alliance. (n.d.). Security.
https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.
https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

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

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 Kysymys 1

Oikea vastaus: A

OPETTAJALLE

Mikä on välimieshyökkäys (Man-in-the-Middle, MitM)? → Kahden osapuolen välisen viestinnän sieppaaminen ja muuttaminen jaetussa verkossa

2 Kysymys 2

Oikea vastaus: A

OPETTAJALLE

Mikä on kaappaustukiasema (Evil Twin)? → Haitallinen Wi-Fi-hotspot, joka on määritetty samalla SSID:llä kuin oikea verkko

3 Kysymys 3

Oikea vastaus: A

OPETTAJALLE

Miten VPN suojaa julkisen Wi-Fi-verkon liikennettä? → Se käärii kaikki verkkopaketit salattuun tunneliin, jolloin nuuskijat eivät pysty lukemaan niitä

4 Kysymys 4

Oikea vastaus: A

OPETTAJALLE

Mitä on pakettien nuuskinta (packet sniffing)? → Laitteisto- tai ohjelmistotyökalujen käyttö verkkopakettien sieppaamiseen ja kirjaamiseen

5 Kysymys 5

Oikea vastaus: A

OPETTAJALLE

Mikä on HTTPS:n tehtävä? → Selaimen ja verkkopalvelimen välisen istuntoliikenteen salaus

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 Kysymys 6 — **Oikea vastaus: Tosi**

OPETTAJALLE

Yhdistyneet käyttäjät voivat helposti kaapata selväkielistä dataa avoimissa julkisissa Wi-Fi-verkoissa.

7 Kysymys 7 — **Oikea vastaus: Epätosi**

OPETTAJALLE

Epätosi: Evil Twin on hyökkääjän pystyttämä luvaton hotspot, joka jäljittelee oikeaa.

8 Kysymys 8 — **Oikea vastaus: Epätosi**

OPETTAJALLE

Epätosi: VPN salaa liikenteen tunnelissa, joten paikalliset nuuskijat eivät voi lukea sitä.

9 Kysymys 9 — **Oikea vastaus: Epätosi**

OPETTAJALLE

Epätosi: HTTPS salaa koko HTTP-viestinnän, myös URL-polun ja sivun sisällön.

10 Kysymys 10 — **Oikea vastaus: Tosi**

OPETTAJALLE

WPA3-suojausta käyttävät Wi-Fi-hotspotit tarjoavat vahvemman suojan kuin avoimet, salasanattomat verkot.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

E 1. SALAKUUNTELU	F 2. NUUSKINTA	D 3. EVIL TWIN	H 4. HTTPS
G 5. VPN	B 6. TUNNELI	A 7. WPA3	C 8. PALOMUURI

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 KAAPPAUS	2 SNIFFAUS	3 EVIL TWIN	4 HTTPS
5 VPN	6 TUNNELI		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 G – WPASUOJAUS	2 C – EVILTWIN	3 B – SNIFFAUS	4 F – TUNNELI
5 H – PALOMUURI	6 A – KAAPPAUS	7 E – VPNYHTEYS	8 D – HTTPS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit SALAKUUNTELU, NUUSKINTA ja EVIL TWIN omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

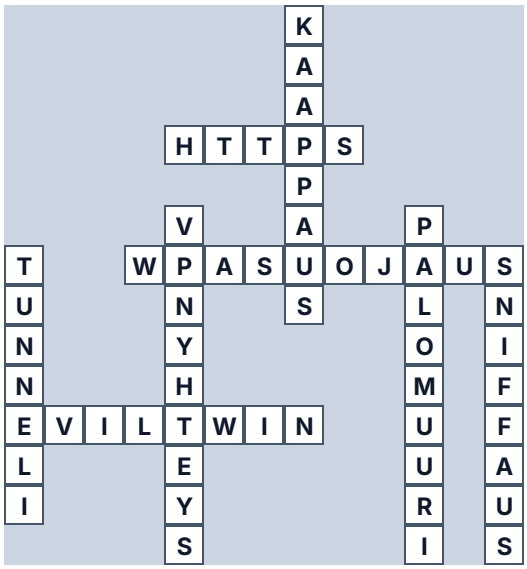
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

2 vaakasuoraan: HTTPS Suojattu verkkoliikenne. (5 kirjainta)

6 vaakasuoraan: WPASUOJAUS Moderni Wi-Fi-suojausstandardi. (10 kirjainta)

8 vaakasuoraan: EVILTWIN Wi-Fi-verkkoa jäljittelevä väärä hotspot. (8 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: KAAPPAUS Liikenteen lukeminen siirron aikana. (8 kirjainta)

3 pystysuoraan: VPNYHTEYS Salattu virtuaalinen yksityisverkko. (9 kirjainta)

4 pystysuoraan: PALOMUURI Saapuvan liikenteen suodatus. (9 kirjainta)

5 pystysuoraan: TUNNELI Suojattu datareitti siirron aikana. (7 kirjainta)

7 pystysuoraan: SNIFFAUS Verkon datapakettien kaappaaminen. (8 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. UPPKAASA — **KAAPPAUS**
2. LENVIWTI — **EVILTWIN**
3. VTHPESYYN — **VPNYHTEYS**
4. OUUSSAJWPA — **WPASUOJAUS**
5. FANSFSUI — **SNIFFAUS**
6. PHTST — **HTTPS**
7. TLEIUNN — **TUNNELI**
8. IMRPOAUUL — **PALOMUURI**

SALAKIRJOITUSHAASTEEN AVAIN

"SALAA JULKISEN WIFIN LIIKENNE VPN LLÄ"

Tapaustutkimusten vastausavain

A Tapaustutkimus 1: Julkisen Wi-Fi-yhteyden pakettinuuskinnan eristäminen

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Julkiseen lentokentän Wi-Fi-verkkoon yhdistetty etämyyntijohtaja huomaa, että useita arkaluonteisia liikesähköposteja vuotaa pian sen jälkeen, kun ne on lähetetty selkokielisinä.
- Suositeltu strategia ja ratkaisu: Edellytä yrityksen VPN-asiakasohjelman käyttöä kaikilla etätyöasemilla. Pakota käyttöön vain HTTPS:ää käyttävät selainlaajennukset ja estä salaamattomat protokollat (kuten HTTP ja FTP) asiakkaan palomuurissa.

B Tapaustutkimus 2: Evil Twin -valehotspotin torjunta

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Hyökkääjät pystyttävät luvattoman langattoman tukiaseman nimeltä "CoffeeShop_Guest", joka jäljittelee oikeaa kahvilan hotspotia ja kaappaa epäilemättömien vieraiden verkkoliikennettä.
- Suositeltu strategia ja ratkaisu: Tarkasta tukiasemien BSSID-MAC-osoitteet verkon aitouden varmistamiseksi. Ota käyttöön asiakkaan tilan validointi, joka estää yhteyden avoimiin verkkoihin, ja vaadi matkapuhelinverkon hotspotteja arkaluonteiseen työhön.