Nimi: _____ Päivämäärä: _____ Pisteet: _____

Kyberturvallisuuden perusteet ja verkkouhat Ennaltaehkäisy

Kyberturvallisuusuhat, verkon palomuurit, monivaiheinen todennus, tietoturvakehykset

KYBERTURVALLISUUDEN PERUSTEIDEN OPPIMISKATSAUS

SUOJATTU
TIETOJEN SALAUS
256-bittinen AES-standardi

LAINMUKAINEN
GLOBAALIT STANDARDIT
GDPR- ja CCPA-säädökset

NOLLALUOTTAMUS
KÄYTTÖKÄYTÄNTÖ
Monivaiheinen tunnistautuminen

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: kyberturvallisuuden perusteiden ja verkkouhkien ehkäisyn perusperiaatteet. Tutustut haittaohjelmauhkiin, monivaiheiseen todennukseen, verkon palomuureihin ja tietoturvapoikkeamiin reagoinnin viitekehyksiin.

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/

Oppimispolkusi: kyberturvallisuuden perusteet

- Tunnista haittaohjelmien, tietojenkalastelun ja yritysverkkoihin tunkeutumisen yleiset reitit.
- Toteuta tavalliset kyberturvallisuuskontrollit, kuten MFA, palomuurit ja päätelaitteiden suojaus.
- Arvioi häiriötilanteiden toimintamenettelyjä tietomurtojen vaikutusten lieventämiseksi.
- Analysoi organisaation riskitekijöitä ja tietoturvan yhdenmukaisuutta NIST-ohjeiden mukaisesti.
- Määritä tietoturvakäytännöt automaattisen credential stuffing -hyökkäyksen lieventämiseksi.

KYBERTURVALLISUUSOPAS: OHJEET

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

KYBERTURVALLISUUDEN PERUSTEET JA UHKIEN TORJUNTA (JOHDANTO)

Kyberturvallisuus suojaa verkkoja, järjestelmiä ja tietoja luvattomilta digitaalisilta hyökkäyksiltä. Vankkojen tietoturvatapojen kehittäminen, palomuurien määrittäminen, monivaiheisen todennuksen vaatiminen ja henkilöstön kouluttaminen uhkien tunnistamiseen ovat yrityksen verkkopuolustuksen olennaisia osia.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. Mikä on tietojenkalasteluhyökkäyksen ensisijainen tavoite?

- A. Tunnistetietojen ja arkaluonteisten käyttäjätietojen varastaminen
- B. Verkkosivuston näkyvyyden parantaminen hakukoneissa
- C. Verkon kaistanleveyden kapasiteetin kasvattaminen
- D. Varmuuskopiodatakeskuksen replikoinnin hallinta

2. Mikä mekanismi tarjoaa vahvimman tilisuojan?

- A. Monitekijätodennus laitteistoavaimilla
- B. Monimutkaiset salasanat, jotka päivitetään kolmenkymmenen päivän välein
- C. Tilille kirjautumisen rajoittaminen työaikaan
- D. Tilin käyttäjätunnuksen piilottaminen julkisista hakemistoista

3. Mikä määrittää kiristysohjelman tartuntakuorman?

- A. Järjestelmätiedostojen salaaminen ja maksun vaatiminen
- B. Näppäinpainallusten hiljainen kirjaaminen etäpalvelimille
- C. Luvattoman mainonnan syöttäminen selaimiin
- D. Paikallisten suoritinresurssien käyttö kryptovaluutan louhintaan

4. Miten nollapäivähaavoittuvuus vaikuttaa suojauksiin?

- A. Se kohdistuu korjaamattomiin, tuntemattomiin haavoittuvuuksiin
- B. Se poistaa yrityksen palomuurin automaattisesti käytöstä
- C. Se pakottaa järjestelmän tekemään kovan uudelleenkäynnistyksen
- D. Sen korjaaminen ei vaadi lainkaan budjettia

5. Mikä viitekehys ohjaa yrityksen tietoturvakontrolleja?

- A. NIST Cybersecurity Framework -ohjeet
- B. W3C:n HTML5-dokumenttiskeemamääritykset
- C. Tulostinajurin asennusoppaat
- D. IETF:n reititysprotokollamääritelmät

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys tf 6

6. Tietojenkalasteluhyökkäykset kohdistuvat vain henkilökohtaisiin sähköpostitileihin.

○ Tosi ○ Epätosi

7 Kysymys tf 7

7. Monivaiheinen tunnistautuminen auttaa estämään tunnuksentäyttöhyökkäyksiä.

○ Tosi ○ Epätosi

8 Kysymys tf 8

8. Palomuurit tarkastavat verkkoliikennettä estääkseen luvattoman porttien käytön.

○ Tosi ○ Epätosi

9 Kysymys tf 9

9. Nollapäivähyökkäysten korjaaminen edellyttää tavallisia virustorjunnan määrittelypäivityksiä.

○ Tosi ○ Epätosi

10 Kysymys tf 10

10. Honeypot on houkutuspalvelin, jolla houkutellaan kyberrikollisia.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Verkon ylläpitäjät asentavat saapuvaa liikennettä suodattavan ratkaisun, jonka nimi on _____ .

2. Hyökkääjä ohittaa järjestelmän korjaukset nollapäivähaavoittuvuuden menetelmällä nimeltä _____ .

3. Hyökkääjät lähettävät väärennettyjä sähköposteja työntekijöille kohdistetuissa _____ -kampanjoissa.

4. Kiristysohjelma on tuhoisa _____ , joka lukitsee käyttäjän tiedot.

5. Vahva salasanojen _____ pienentää tunnistetietojen varastamisen riskiä.

6. Arkaluonteisen viestinnän suojaamiseksi käyttäjät soveltavat _____ -protokollia.

SANASTON SANAPANKKI

HAITTAOHJELMA HYGIENIA HYVÄKSIKÄYTTÖ MONIVAIHEINEN NOLLAPÄIVÄ
PALOMUURI SALAUS TIETOJENKALASTELU

Kirjoita vastauksesi tähän:

1. **2.**

3. **4.**

5. **6.**

Tarkistuspiste 4: Tietoturvakäsitteiden yhdistäminen

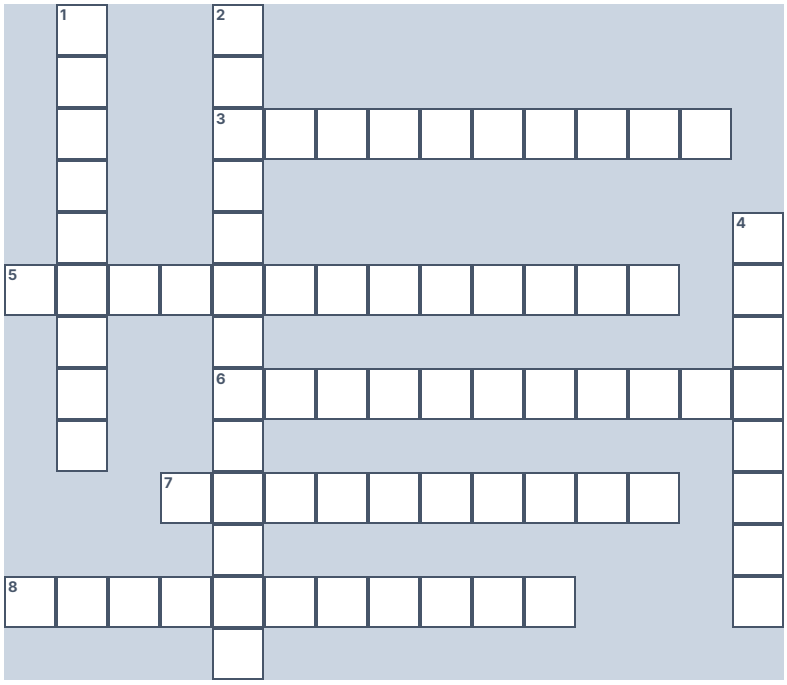
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. Kiristysohjelmauhka	A	Jäsennellyt ohjeistot, kuten NIST, joita käytetään kyberriskien hallintaan.
☐	2. Monivaiheinen todennus	B	Jäsennelty suunnitelma tietoturvaloukkausten käsittelyyn ja lieventämiseen.
☐	3. Nollapäivähyökkäys	C	Verkkoeste, joka suodattaa liikennettä suojaussääntöjen perusteella.
☐	4. Houkutuspoletti	D	Haittaohjelma, joka salaa tiedot ja vaatii rahaa purkamisesta.
☐	5. Tunkeutumispalomuuri	E	Haavoittuvuuden hyväksikäyttö, joka kohdistetaan ennen kuin valmistaja julkaisee korjauksen.
☐	6. Poikkeamiin reagointi	F	Parhaat käytännöt tunnistetietojen ja todennusavainten hallintaan.
☐	7. Salasanahygienia	G	Tietoturvatarkistus, joka edellyttää kahta tai useampaa todennustekijää.
☐	8. Tietoturvakehys	H	Houkutusjärjestelmä, joka on pystytetty houkuttelemaan ja analysoimaan haitallisia toimijoita.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

3. Haavoittuvuuden hyväksikäyttö, joka kohdistuu ennen toimittajan korjauksen julkaisua (10)

5. Haittaohjelma, joka salaa tiedot ja vaatii rahallista maksua salauksen purkamisesta (13)

6. Houkutusjärjestelmä, joka perustetaan houkuttelemaan ja analysoimaan haitallisia toimijoita (11)

7. Jäsennellyt ohjeet, kuten NIST, joita käytetään kyberriskien hallintaan (10)

8. Jäsennelty suunnitelma tietoturvaloukkausten käsittelyyn ja lieventämiseen (11)

PYSTYSUORAAN

1. Verkon suoja, joka suodattaa liikennettä tietoturvasääntöjen perusteella (9)

2. Tietoturvan varmennus, joka edellyttää kahta tai useampaa todennustekijää (13)

4. Parhaat käytännöt tunnistetietojen ja todennusavainten hallintaan (8)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

3 vaakasuoraan: Haavoittuvuuden hyväksikäyttö, joka kohdistuu ennen toimittajan korjauksen julkaisua (10 kirjainta):

5 vaakasuoraan: Haittaohjelma, joka salaa tiedot ja vaatii rahallista maksua salauksen purkamisesta (13 kirjainta):

6 vaakasuoraan: Houkutusjärjestelmä, joka perustetaan houkuttelemaan ja analysoimaan haitallisia toimijoita (11 kirjainta):

7 vaakasuoraan: Jäsennellyt ohjeet, kuten NIST, joita käytetään kyberriskien hallintaan (10 kirjainta):

8 vaakasuoraan: Jäsennelty suunnitelma tietoturvaloukkausten käsittelyyn ja lieventämiseen (11 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Verkon suoja, joka suodattaa liikennettä tietoturvasääntöjen perusteella (9 kirjainta):

2 pystysuoraan: Tietoturvan varmennus, joka edellyttää kahta tai useampaa todennustekijää (13 kirjainta):

4 pystysuoraan: Parhaat käytännöt tunnistetietojen ja todennusavainten hallintaan (8 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

LUNNASOHJELMA, MONIVAIHEINEN, NOLLAPÄIVÄ, HUNAJAPOTTI, PALOMUURI, VASTETOIMET, HYGIENIA, VIITEKEHYS

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. LUNNASOHJELMA**
- **B. MONIVAIHEINEN**
- **C. NOLLAPÄIVÄ**
- **D. HUNAJAPOTTI**
- **E. PALOMUURI**
- **F. VASTETOIMET**
- **G. HYGIENIA**
- **H. VIITEKEHYS**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Verkon suoja, joka suodattaa liikennettä tietoturvasääntöjen perusteella.
2. Jäsennelty suunnitelma tietoturvaloukkausten käsittelyyn ja lieventämiseen.
3. Haittaohjelma, joka salaa tiedot ja vaatii rahallista maksua salauksen purkamisesta.
4. Tietoturvan varmennus, joka edellyttää kahta tai useampaa todennustekijää.
5. Parhaat käytännöt tunnistetietojen ja todennusavainten hallintaan.
6. Jäsennellyt ohjeet, kuten NIST, joita käytetään kyberriskien hallintaan.
7. Haavoittuvuuden hyväksikäyttö, joka kohdistuu ennen toimittajan korjauksen julkaisua.
8. Houkutusjärjestelmä, joka perustetaan houkuttelemaan ja analysoimaan haitallisia toimijoita.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. ONJMSUHELLAAN
2. VLNOAÄÄIPL
3. PUMAUIORL
4. IIANEHYG
5. ENONHVNAIIMEI
6. JIAOTTHUPNA
7. IEVAOTMEST
8. YTKSVEIEHI

Bonustehtävä: Nopeat vastaukset

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

1	Kyberturvallisuuden ammatteja			
2	Syitä päivittää ohjelmistot			
3	Asioita, jotka palomuuri voi estää			
4	Varoitusmerkkejä sähköpostissa			
5	Asioita, joista otat varmuuskopion			
6	Tunnettuja kyberhyökkäystyyppejä			
7	Asioita, joita hunajapurkki voi houkutella			
8	Tietoja, joita sinun ei pitäisi koskaan jakaa			
9	Merkkejä siitä, että tietokone on saanut tartunnan			
10	Hakkereista kertovia elokuvia tai sarjoja			
11	Tietoturvakerroksia, joita voit rakentaa			
12	Asioita, joita harjoitellaan tietoturvaharjoituksessa			
13	Tietoturvatyökaluja, jotka tunnet			
14	Ihmisiä, joilta voit pyytää IT-apua			
15	Sanoja, jotka alkavat sanalla "kyber"			

Tarkistuspiste 8: Kyberturvallisuuden tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: LUNNASOHJELMASTA PALAUTUMISEN STRATEGIA

👷

Tilanne: Yrityksen verkko on saanut kiristyshaittaohjelmatartunnan, joka lukitsee kriittiset tietokannat. Hyökkääjät vaativat 100 000 dollarin kryptovaluuttamaksua. Yrityksellä on offline-varmuuskopiot 24 tunnin takaa.

Keskustelukysymys: Analysoi maksamisen riskit ja arvioi palautumisstrategia.

TAPAUSTUTKIMUS 2: CREDENTIAL STUFFING -HYÖKKÄYSTEN TORJUNTA

👷

Tilanne: Verkkopalveluun kohdistuu tunnuksentäyttöhyökkäys, jossa hakkerit testaavat miljoonia muilta sivustoilta varastettuja käyttäjätunnus–salasana-pareja.

Keskustelukysymys: Kuvaile tämän hyökkäyksen toimintatapa yksityiskohtaisesti ja esitä kaksi puolustusjärjestelmää.

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	21	15	10	1	1		10	28	18	10	5	19	20	5	12	13	28

13	15	14	9	22	1	9	8	5	9	19	5	12	12	1

20	15	4	5	14	14	21	11	19	5	12	12	1

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 kyberturvallisuuden päätavoite?

Päätavoite on suojata verkkoja, laitteita ja tietoja luvattomalta käytöltä, hyökkäyksiltä ja vahingossa tapahtuvilta vahingoilta.

Q2: Miten tietojenkalastelu eroaa kohdennetusta tietojenkalastelusta?

Tietojenkalastelu on laaja satunnaisiin käyttäjiin kohdistuva sähköpostikampanja, kun taas kohdennettu tietojenkalastelu (spear phishing) kohdistuu tiettyihin henkilöihin henkilökohtaisten tietojen avulla.

Q3: Mikä on verkkopalomuuri?

Palomuuri on verkon suojausjärjestelmä, joka valvoo ja suodattaa saapuvaa ja lähtevää liikennettä ennalta määriteltyjen suojaussääntöjen perusteella.

Q4: Miksi monivaiheinen todennus (MFA) on tarpeen?

MFA lisää tärkeän suojakerroksen ja estää pääsyn, vaikka hyökkääjät varastaisivat tai murtaisivat ensisijaisen salasanan.

Q5: Mikä määrittelee tietokonevirukset?

Virus on itseään kopioiva haittaohjelma, joka liittyy puhtaisiin tiedostoihin ja leviää järjestelmissä suoritettuaan.

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

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q6: Miten kiristyshaittaohjelma lukitsee paikalliset tiedot?

Kiristyshaittaohjelma käyttää salausalgoritmeja käyttäjän tiedostojen salaamiseen, jolloin ne ovat lukukelvottomia, kunnes salauksenpurkuavain annetaan.

Q7: Mikä on nollapäivähaavoittuvuus?

Nollapäivähaavoittuvuus on ohjelmiston tietoturva-aukko, joka on toimittajalle tuntematon, jolloin korjaustiedoston kehittämiseen ei jää aikaa ennen hyväksikäyttöä.

Q8: Mikä rooli NIST-viitekehyksellä on?

NIST-viitekehys tarjoaa vapaaehtoisia ohjeita ja standardeja, jotka auttavat organisaatioita hallitsemaan ja pienentämään kyberturvallisuusriskejä.

Q9: Mikä on tietoturvapoikkeamien toimintasuunnitelma?

Se on dokumentoitu menettelyjoukko tietoturvaloukkausten ja verkon vaarantumisen havaitsemiseen, rajaamiseen ja niistä toipumiseen.

Q10: Miten sosiaalinen manipulointi hyödyntää käyttäjiä?

Sosiaalinen manipulointi käyttää psykologista vaikuttamista huijatakseen työntekijät paljastamaan salasanoja tai lataamaan haitallisia tiedostoja.

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

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

Q1: Miten DDoS-hyökkäys ylikuormittaa verkkopalvelimet?

DDoS-hyökkäys koordinoi miljoonia kaapattuja bottiverkon laitteita tulvittamaan palvelimen liikenteellä, mikä kuluttaa kaistanleveyden ja suorittimen rajat.

Q2: Mikä ero on symmetrisellä ja epäsymmetrisellä salauksella?

Symmetrinen salaus käyttää yhtä avainta salaukseen ja purkamiseen, kun taas epäsymmetrinen salaus käyttää julkisen ja yksityisen avaimen paria.

Q3: Miten hakkerit toteuttavat SQL-injektiohyökkäyksiä?

Hyökkääjät syöttävät lomakekenttiin haitallisia SQL-komentoja ja huijaavat taustatietokannan luovuttamaan luvattomia käyttäjätietoja.

Q4: Mitä sivuttaisliike on verkkomurroissa?

Se on tekniikka, jossa hyökkääjät hyödyntävät alkuperäistä palvelinpääsyä vaarantaakseen muita sisäverkon toisiinsa kytkettyjä järjestelmiä.

Q5: Miten DNS-väärennös ohjaa verkkoliikennettä uudelleen?

DNS-huijaus muuttaa nimipalvelimen välimuistin tietueita ja ohjaa oikeat käyttäjät haitallisille, kohdeverkkotunnuksia muistuttaville sivustoille.

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

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

Q6: Mikä on laitteistopohjainen suojaustunniste?

Se on fyysinen laite (kuten YubiKey), joka tuottaa kryptografisia todennustodisteita ja tarjoaa parhaan suojan etätietojenkalastelua vastaan.

Q7: Miten tietoturvatiimit käyttävät houkutuspönttejä (honeypot)?

Tiimit ottavat käyttöön ei-tuotannollisia houkutuspalvelimia havaitakseen tunkeutumiset varhain ja analysoidakseen luvattomien toimijoiden hyökkäyskuvioita.

Q8: Mikä on vähimpien oikeuksien periaate?

Se on tietoturvastandardi, jossa käyttäjien käyttöoikeudet rajoitetaan ehdottomaan vähimmäismäärään, joka tarvitaan heidän työroolinsa hoitamiseen.

Q9: Miten välimieshyökkäys (Man-in-the-Middle) hyödyntää yhteyksiä?

Hyökkääjä sieppaa ja muuttaa kahden laitteen välistä viestintää salaamattomissa verkoissa ja varastaa istuntotunnuksia ja tunnistetietoja.

Q10: Mitä ovat vaarantumisen indikaattorit (IOC)?

IOC-tunnisteet ovat rikosteknisiä vihjeitä, kuten epätavalliset rekisterimuutokset tai luvaton IP-liikenne, jotka osoittavat järjestelmään murtauduttavan.

Osa 11: 10 tosielämän kyberturvallisuusfaktaa ja havaintoa

Tutustu todellisiin tosiasioihin tietoturvaloukkauksista, puolustusmekanismeista ja vaatimustenmukaisuusstandardeista.

1. TURVALLISUUSOIVALLUS

Hyökkääjät skannaavat jatkuvasti internetiä haavoittuvien palvelimien löytämiseksi ja lähettävät tietojenkalasteluviestejä työntekijöiden sähköpostiin.

2. TURVALLISUUSOIVALLUS

Inhimillinen virhe, kuten tietojenkalastelulinkkien napsauttaminen, on yleinen tekijä tietomurroissa, minkä vuoksi koulutus on tärkeää.

3. TURVALLISUUSOIVALLUS

Tietomurron kustannuksiin kuuluvat oikeudelliset sakot, asiakaskato sekä tutkinta ja korjaus, ja ne voivat nousta miljooniin dollareihin.

4. TURVALLISUUSOIVALLUS

Tietojenkalasteluun kestävä MFA, kuten laitteistoturva-avaimet, on vahvin MFA-tyyppi ja CISA:n painottama standardi. [2]

5. TURVALLISUUSOIVALLUS

Kiristyshaittaohjelmat ovat edelleen merkittävä uhka yritysverkoille, ja CISA suosittelee offline-tilassa säilytettäviä salattuja varmuuskopioita keskeisenä puolustuksena. [4]

6. TURVALLISUUSOIVALLUS

NIST Cybersecurity Framework 2.0 (2024) sisältää kuusi ydintoimintoa: Govern, Identify, Protect, Detect, Respond, Recover. [1]

7. TIETOTURVATIETOA

Credential stuffing -botit testaavat vuotaneita käyttäjätunnus- ja salasanapareja massana pankki- ja verkkokauppojen kirjautumisportaaleissa.

8. TIETOTURVATIETOA

Nollapäivähaavoittuvuuksien markkinoita on maailmanlaajuisesti, ja vakavia haavoittuvuuksia voidaan myydä suurilla summilla ennen kuin ne korjataan.

9. TIETOTURVATIETOA

Houkutusjärjestelmä (honeypot) ilmoittaa tunkeutumishälytyksistä heti, koska oikeilla käyttäjillä ei ole syytä käyttää sitä.

10. TURVALLISUUSOIVALLUS

Transport Layer Security (TLS) salaa selainistunnot ja estää pakettien nuuskimisen julkisissa Wi-Fi-verkoissa.

Tekniset viitteet ja lähteet

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

TIETEELLISET JA ALAN VIITTEET

[1] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] 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

[4] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

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

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 **Tietojenkalasteluhyökkäykset** TIETOJENKALASTELU — **Oikea vastaus: A**

OPETTAJALLE

Tietojenkalastelukampanjat yrittävät varastaa tunnistetietoja ja arkaluonteisia käyttäjätietoja väärennettyjen sähköpostien avulla. Lähde: OWASP Secure Configuration.

2 **Tilin suojaus** MFA-AVAIN — **Oikea vastaus: A**

OPETTAJALLE

Laitteistotunnisteita käyttävä monivaiheinen tunnistautuminen (MFA) tarjoaa vahvimman suojan tilin käyttöä vastaan. Lähde: NIST Digital Identity.

3 **Kiristyshaittaohjelmauhka** KIRISTYSHAITTAOHJELMA — **Oikea vastaus: A**

OPETTAJALLE

Kiristyshaittaohjelma salaa kriittisiä järjestelmiä ja tietoja ja vaatii kryptovaluuttamaksua salauksenpurkuavaimista. Lähde: Center for Internet Security (CIS).

4 **Nollapäivähaavoittuvuus** NOLLAPÄIVÄ — **Oikea vastaus: A**

OPETTAJALLE

Nollapäivähaavoittuvuudet hyödyntävät korjaamattomia, tuntemattomia tietoturva-aukkoja ennen kuin valmistajan korjaus on saatavilla. Lähde: OWASP Secure Configuration.

5 **Tietoturvakehykset** VIITEKEHYKSET — **Oikea vastaus: A**

OPETTAJALLE

NIST:n kaltaiset viitekehykset tarjoavat jäsenneltyjä ohjeita, jotka voivat auttaa organisaatioita hallitsemaan ja vähentämään kyberriskejä. Lähde: NIST Digital Identity.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Kohdennettu tietojenkalastelu** TIETOJENKALASTELU

Oikea vastaus: Epätosi

OPETTAJALLE

Tietojenkalasteluhyökkäykset kohdistuvat sekä yritysverkkoihin että henkilökohtaisiin tileihin hyökkäysreittien laajentamiseksi. Lähde: OWASP Secure Configuration.

7 **Kysymys 7**

Oikea vastaus: Tosi

OPETTAJALLE

Monivaiheinen tunnistautuminen vaatii toisen tekijän, joten varastettu salasana yksinään ei yleensä riitä kirjautumiseen.

8 **Liikenteen palomuuri** PALOMUURI

Oikea vastaus: Tosi

OPETTAJALLE

Palomuurit tarkastavat ja estävät liikennettä tietyissä verkkoporteissa suodattaakseen pois luvattomat yhteydet. Lähde: Center for Internet Security (CIS).

9 **Nollapäivähaavoittuvuuteen reagointi** NOLLAPÄIVÄ

Oikea vastaus: Epätosi

OPETTAJALLE

Nollapäivähaavoittuvuuksien korjaaminen edellyttää koodikorjauksia ja WAF-suodatusta, koska allekirjoituksia ei vielä ole. Lähde: OWASP Secure Configuration.

10 **Houkutushoneypotit** HUNAJAPURKKI

Oikea vastaus: Tosi

OPETTAJALLE

Hunajapurkit ovat harhauttavia palvelimia, joiden avulla tietoturvatiimit houkuttelevat, hälyttävät ja tutkivat haitallisia toimijoita. Lähde: Center for Internet Security (CIS).

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

D 1. Kiristysohjelmauhka	G 2. Monivaiheinen todennus	E 3. Nollapäivähyökkäys	H 4. Houkutuspoletti
C 5. Tunkeutumispalomuuri	B 6. Poikkeamiin reagointi	F 7. Salasanahygienia	A 8. Tietoturvakehys

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 PALOMUURI	2 HYVÄKSIKÄYTTÖ	3 TIETOJENKALASTELU	4 HAITTAOHJELMA
5 HYGIENIA	6 SALAUS		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 E – PALOMUURI	2 F – VASTETOIMET	3 A – LUNNASOHJELMA	4 B – MONIVAIHEINEN
5 G – HYGIENIA	6 H – VIITEKEHYS	7 C – NOLLAPÄIVÄ	8 D – HUNAJAPOTTI

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit Kiristysohjelmauhka, Monivaiheinen todennus ja Nollapäivähyökkäys omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

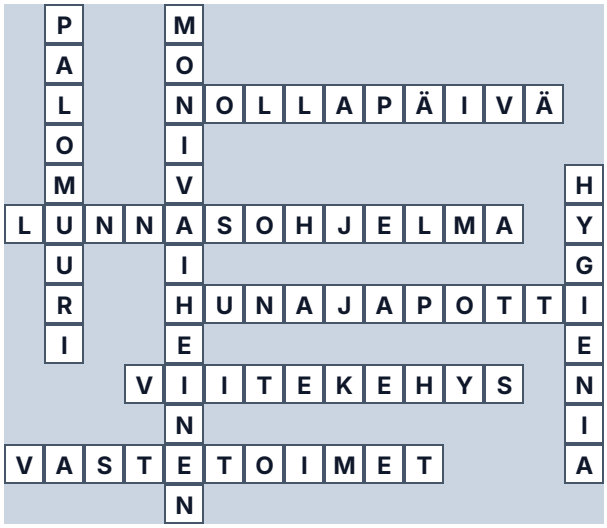
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

3 vaakasuoraan: NOLLAPÄIVÄ Haavoittuvuuden hyväksikäyttö, joka kohdistuu ennen toimittajan korjauksen julkaisua (10 kirjainta)

5 vaakasuoraan: LUNNASOHJELMA Haittaohjelma, joka salaa tiedot ja vaatii rahallista maksua salauksen purkamisesta (13 kirjainta)

6 vaakasuoraan: HUNAJAPOTTI Houkutusjärjestelmä, joka perustetaan houkuttelemaan ja analysoimaan haitallisia toimijoita (11 kirjainta)

7 vaakasuoraan: VIITEKEHYS Jäsennellyt ohjeet, kuten NIST, joita käytetään kyberriskien hallintaan (10 kirjainta)

8 vaakasuoraan: VASTETOIMET Jäsennelty suunnitelma tietoturvaloukkausten käsittelyyn ja lieventämiseen (11 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: PALOMUURI Verkon suoja, joka suodattaa liikennettä tietoturvasääntöjen perusteella (9 kirjainta)

2 pystysuoraan: MONIVAIHEINEN Tietoturvan varmennus, joka edellyttää kahta tai useampaa todennustekijää (13 kirjainta)

4 pystysuoraan: HYGIENIA Parhaat käytännöt tunnistetietojen ja todennusavainten hallintaan (8 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. ONJMSUHELLAAN — **LUNNASOHJELMA**
2. VLNOAÄÄIPL — **NOLLAPÄIVÄ**
3. PUMAUIORL — **PALOMUURI**
4. IIANEHYG — **HYGIENIA**
5. ENONHVNAIIMEI — **MONIVAIHEINEN**
6. JIAOTTHUPNA — **HUNAJAPOTTI**
7. IEVAOTMESTT — **VASTETOIMET**
8. YTKSVEIEHI — **VIITEKEHYS**

SALAKIRJOITUSHAASTEEN AVAIN

"SUOJAA JÄRJESTELMÄ MONIVAIHEISELLA TODENNUKSELLA"

Tapaustutkimusten vastausavain

A Tapaustutkimus 1: Lunnasohjelmasta palautumisen strategia

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Yrityksen verkko on saanut kiristysohjelmatartunnan, joka lukitsee kriittisiä tietokantoja. Hyökkääjät vaativat 100 000 dollarin kryptovaluuttamaksua. Yrityksellä on offline-varmuuskopiot 24 tunnin takaa.
- Suositeltu strategia ja ratkaisu: Maksamisen riskit: Maksaminen ei takaa tiedostojen salauksen purkua, leimaa yrityksen maksavaksi kohteeksi ja rahoittaa rikollista toimintaa. Palautusstrategia: Tiimin tulee eristää tartunnan saaneet isännät, tyhjentää vaarantuneet palvelimet ja palauttaa tiedot offline-varmuuskopioista. Heidän on korjattava alkuperäinen pääsyreitti (tietojenkalastelu tai haavoittuvuuden hyväksikäyttö) välittömän uudelleentartunnan estämiseksi.

B Tapaustutkimus 2: Credential stuffing -hyökkäysten torjunta

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Verkkopalveluun kohdistuu tunnuksentäyttöhyökkäys (credential stuffing), jossa hakkerit kokeilevat miljoonia muilta sivustoilta varastettuja käyttäjätunnus- ja salasanapareja.
- Suositeltu strategia ja ratkaisu: Mekanismi: Hyökkääjät hyödyntävät salasanojen uudelleenkäyttöä eri sivustoilla ja kirjautuvat käyttäjätileille automaattisten bottien avulla. Puolustukset: 1. Monivaiheinen tunnistautuminen (MFA) estää kirjautumisyritykset, vaikka salasana olisi oikein. 2. Nopeusrajoitusten ja CAPTCHA-testien käyttöönotto estää automaattista bottiliikennettä tulvittamasta kirjautumispisteitä.