Nimi: _____ Päivämäärä: _____ Pisteet: _____

Salasanavuodot ja tunnistetietojen turvallisuus

Credential stuffing, tietomurrot, tiivistealgoritmit, monivaiheinen todennus ja salasanojen turvallisuus.

SALASANAVUODOT, OPPIMISKATSAUS

SUOJATTU
TIETOJEN SALAUS
256-bittinen AES-standardi

LAINMUKAINEN
GLOBAALIT STANDARDIT
GDPR- ja CCPA-säädökset

NOLLALUOTTAMUS
KÄYTTÖKÄYTÄNTÖ
Monivaiheinen tunnistautuminen

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: salasanavuodot ja tunnistetietojen turvallisuus. Tutustut tunnistetietojen täyttöhyökkäyksiin (credential stuffing), tietomurtoihin, tiivistealgoritmeihin, monivaiheiseen todennukseen ja salasanahallintaohjelmiin.

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/salasanat-vuotivat/

Oppimispolkusi: salasanojen turvallisuus

- Ymmärrä tunnistetietojen paljastumisen riskit pimeän verkon foorumeilla.
- Toteuta monivaiheinen tunnistautuminen (MFA) ja vuotaneiden tunnistetietojen valvonta.
- Suunnittele yrityksen tietoturvapuolustuksia kohdennettuja sosiaalisen manipuloinnin huijauksia vastaan.

SALASANAVUOTOJEN OPAS, OHJEET

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

SALASANAVUODOT JA TUNNISTETIETOJEN TURVALLISUUS (JOHDANTO)

Salasanavuodot paljastavat käyttäjien tunnistetietoja julkisilla sivustoilla ja pimeässä verkossa. Salasananhallinnan yksilölliset salasanat, vuotaneiden salasanojen tarkistus ja monivaiheinen tunnistautuminen (MFA) pienentävät tunnistetietojen täyttöhyökkäysten riskiä, kun taas suolattu ja hidas salasanojen tiivistys rajoittaa vahinkoa, jos salasanatietokanta varastetaan.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1 **1. Mitä on tunnusten täyttöhyökkäys (credential stuffing)?**

- A. Automaation käyttö vuotaneiden käyttäjätunnus- ja salasanayhdistelmien testaamiseen usealla sivustolla
- B. Paikallisten tietokantojen tallennustiedostojen salaaminen
- C. Verkkopalvelinten ylikuormittaminen verkkoliikennepyynnöillä
- D. Näppäinsyötteiden salainen valvonta

2 **2. Minkä algoritmin OWASP luettelee ensisijaiseksi valinnaksi salasanojen tallentamiseen nykyään?**

- A. Argon2id
- B. MD5
- C. SHA-1
- D. ROT13

3 **3. Miten monivaiheinen tunnistautuminen (MFA) pienentää salasanavuotojen riskiä?**

- A. Se vaatii lisävarmistustekijän, joten varastettu salasana yksinään ei riitä
- B. Se vaihtaa salasanan automaattisesti tunnin välein
- C. Se salaa käyttäjätunnuksen siirron aikana
- D. Se ilmoittaa luottotietoyritykselle vilpillisistä pyynnöistä

4 **4. Mikä on tietomurtovedos?**

- A. Kokoelma vuotaneita käyttäjien tunnistetietoja, jotka on julkaistu verkossa tai myyty hakkerifoorumeilla
- B. Tietokantatiedostojen varmuuskopio, joka on tallennettu toiseen paikkaan
- C. Verkkopalvelimen lokien väliaikainen välimuisti
- D. Ylläpitotyökalu, jolla nollataan käyttäjien salasanoja

5 **5. Mikä on salasanojen hallintaohjelman tehtävä?**

- A. Yksilöllisten, vahvojen salasanojen luominen ja tallentaminen jokaiselle tilille
- B. Verkkoliikenteen valvonta salasanavuotojen varalta
- C. Automaattisten brute force -hyökkäysten estäminen yhdyskäytävässä
- D. Tietokannan tallennuslohkojen skannaus salaamattomien salasanojen varalta

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Salasanojen käyttäminen uudelleen useilla tileillä lisää tunnustäytön riskiä.

○ Tosi ○ Epätosi

7 Kysymys 7

7. SHA-1 on suositeltu tiivistefunktio nykyaikaiseen salasanojen tallennukseen.

○ Tosi ○ Epätosi

8 Kysymys 8

8. Pelkkä salasanan monimutkaisuuden pakottaminen (ilman monivaiheista tunnistautumista) estää tunnistetietojen täyttöhyökkäykset täysin.

○ Tosi ○ Epätosi

9 Kysymys 9

9. Pimeän verkon seurantatyökalut skannaavat internetiä yrityksen vaarantuneiden kirjautumistietojen varalta.

○ Tosi ○ Epätosi

10 Kysymys 10

10. Suolatut tiivisteet lisäävät salasanoihin yksilöllistä satunnaisdataa ennen tiivistämistä sateenkaaritaulu-hyökkäysten torjumiseksi.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Vuotaneiden tunnistetietojen testaaminen monissa verkkosovelluksissa on tunnistetietojen _____ .

2. OWASP:n yhä hyväksymä hidas, mukautuva salasanojen tiivistysalgoritmi on _____ .

3. Luottamuksellisten tietokantatiedostojen paljastuminen internetiin on _____ .

4. Satunnaisten arvojen lisääminen salasanoihin ennen tiivistämistä on nimeltään _____ .

5. Käyttäjätunnusten turvallinen paikallinen tietokanta on salasanojen _____ .

6. Toisen kirjautumisen varmistusvaiheen lisäävä menetelmä on _____ .

SANASTON SANAPANKKI

BCRYPT HALLINNOIJA KALASTELU MFA-TUNNISTUS RAINBOW-TAULU SUOLAUS TIETOMURTO TÄYTTÖHYÖKKÄYS

Kirjoita vastauksesi tähän:

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

Tarkistuspiste 4: Tietoturvakäsitteiden yhdistäminen

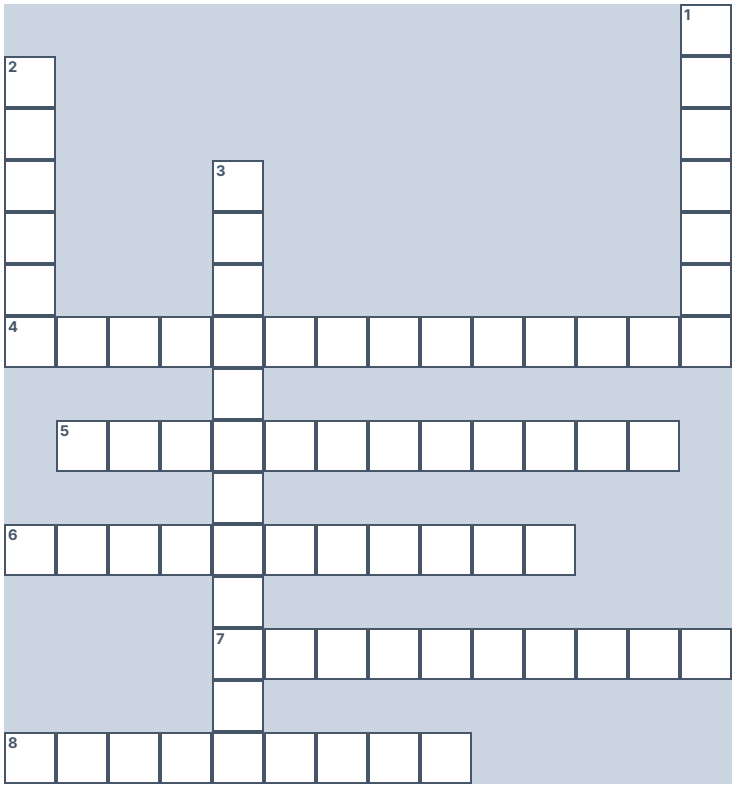
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. TUNNUSTÄYTTÖ	A	Ennalta laskettu salasanatiivisteiden taulukko.
☐	2. BCRYPT	B	Monivaiheinen kirjautumistarkistus.
☐	3. TIETOMURTO	C	Käyttötunnusten tallennustyökalu.
☐	4. SUOLAUS	D	Luvaton tietokannan paljastuminen.
☐	5. HALLINTA	E	Sosiaalinen manipulointi tunnusten varastamiseksi.
☐	6. MFA	F	Vuotaneiden tunnusten testaus.
☐	7. RAINBOW-TAULU	G	Satunnaisen suolan lisääminen salasanatiivisteeseen.
☐	8. TIETOJENKALASTELU	H	Hidas salasanan tiivistysalgoritmi.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

4. Vuotaneiden tunnistetietojen testaaminen. (14)

5. Valmiiksi laskettu salasanatiivisteiden taulukko. (12)

6. Tunnistetietojen tallennustyökalu. (11)

7. Tietokannan luvaton paljastuminen. (10)

8. Sosiaalinen manipulointi kirjautumistietojen varastamiseksi. (9)

PYSTYSUORAAN

1. Satunnaisen suolan lisääminen salasanan tiivisteeseen. (7)

2. Hidas salasanojen tiivistysalgoritmi. (6)

3. Monivaiheinen kirjautumisen tarkistus. (12)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

4 vaakasuoraan: Vuotaneiden tunnistetietojen testaaminen. (14 kirjainta):

5 vaakasuoraan: Valmiiksi laskettu salasanatiivisteiden taulukko. (12 kirjainta):

6 vaakasuoraan: Tunnistetietojen tallennustyökalu. (11 kirjainta):

7 vaakasuoraan: Tietokannan luvaton paljastuminen. (10 kirjainta):

8 vaakasuoraan: Sosiaalinen manipulointi kirjautumistietojen varastamiseksi. (9 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Satunnaisen suolan lisääminen salasanan tiivisteeseen. (7 kirjainta):

2 pystysuoraan: Hidas salasanojen tiivistysalgoritmi. (6 kirjainta):

3 pystysuoraan: Monivaiheinen kirjautumisen tarkistus. (12 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

TÄYTTÖHYÖKKÄYS BCRYPT TIETOMURTO SUOLAUS HALLINNOIJA
MFATUNNISTUS RAINBOWTAULU KALASTELU

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. TÄYTTÖHYÖKKÄYS**
- **B. BCRYPT**
- **C. TIETOMURTO**
- **D. SUOLAUS**
- **E. HALLINNOIJA**
- **F. MFATUNNISTUS**
- **G. RAINBOWTAULU**
- **H. KALASTELU**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Sosiaalinen manipulointi kirjautumistietojen varastamiseksi.
2. Tietokannan luvaton paljastuminen.
3. Hidas salasanojen tiivistysalgoritmi.
4. Valmiiksi laskettu salasanatiivisteiden taulukko.
5. Vuotaneiden tunnistetietojen testaaminen.
6. Satunnaisen suolan lisääminen salasanan tiivisteeseen.
7. Tunnistetietojen tallennustyökalu.
8. Monivaiheinen kirjautumisen tarkistus.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. KÖYKHYÄÖÄT YSTT
2. TTTIOOURME
3. HNNOLAJAIIL
4. LTBIWUOUAR AN
5. YRTBPC
6. UOASLSU
7. ISUMFNSTUA NT
8. USLKAATEL

Bonustehtävä: Nopeat vastaukset

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

1	Turvallisia tapoja, joita voit aloittaa tänään			
2	Vahvan salasanan sääntöjä			
3	Salasanahallintoja, jotka tunnet			
4	Tietoturvatyökaluja, jotka tunnet			
5	Varoitusmerkkejä sähköpostissa			
6	Hauskoja sanoja pitkään salasanalauseeseen			
7	Tapoja kirjautua ilman salasanaa			
8	Tietoja, joita sinun ei pitäisi koskaan jakaa			
9	Syitä päivittää ohjelmistot			
10	Asioita, joita teet, kun salasana vuotaa			
11	Tilejä, jotka tarvitsevat monivaiheisen tunnistautumisen			
12	Paikkoja, joihin salasanoja ei pitäisi koskaan tallentaa			
13	Merkkejä siitä, että tietokone on saanut tartunnan			
14	Huonoja salasanoja, joita ihmiset käyttävät			
15	Asioita, joista otat varmuuskopion			

Tarkistuspiste 8: Kyberturvallisuuden tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: YRITYKSEN KÄYTTÖTUNNUSVUODON KORJAAMINEN



Tilanne: Pimeän verkon valvontapalvelu varoittaa organisaatiota siitä, että tietokantavedos, joka sisältää yrityksen järjestelmänvalvojien salasanoja, on julkaistu verkossa.

Keskustelukysymys: Analysoi tunnusvuodon riskit ja ehdota hallinnollista nollausstrategiaa.

TAPAUSTUTKIMUS 2: SALASANOJEN TIIVISTÄMISSTANDARDIEN TOTEUTTAMINEN



Tilanne: Yrityksen tietokanta tallentaa tällä hetkellä käyttäjien salasanat vanhentuneilla MD5-tiivisteillä ilman kryptografista suolaa, mikä tekee niistä alttiita nopealle poimimiselle.

Keskustelukysymys: Suunnittele siirtostrategia tietokannan tiivistealgoritmin päivittämiseksi.

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		22	21	15	20	1	14	5	5	20

19	1	12	1	19	1	14	1	20		13	6	1

20	21	14	14	9	19	20	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 salasanavuoto?

Salasanavuoto syntyy, kun käyttäjien kirjautumistiedot paljastuvat tietomurtojen tai palvelinten virheellisten määritysten kautta.

Q2: Miten hakkerit löytävät vuotaneita salasanoja?

Hakkerit selaavat pimeän verkon keskustelupalstoja, julkisia tietokantavuotoja ja liitesivustoja, joilla tietomurtojen tietoja julkaistaan [8].

Q3: Onko salasanan uudelleenkäyttö vaarallista?

Kyllä, koska jos yksi sivusto vaarantuu, hakkerit voivat kokeilla samoja tunnuksia tuhansilla muilla alustoilla [3].

Q4: Mikä on kryptografinen suola?

Suola (salt) on satunnaista dataa, joka lisätään salasanaan ennen tiivistämistä, mikä tekee valmiiksi laskettuihin hakutauluihin perustuvista hyökkäyksistä tehottomia [2].

Q5: Miksi MD5 on vanhentunut?

MD5 on nopea, vanhentunut yleiskäyttöinen tiiviste, joten hyökkääjät voivat testata salasana-arvauksia erittäin nopeasti, etenkin kun tiivisteisiin ei ole lisätty suolaa [2].

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

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q6: Miten salasanojen hallintaohjelma suojaa käyttäjiä?

Se luo automaattisesti monimutkaiset, yksilölliset tunnistetiedot jokaiselle sivustolle, mikä vähentää inhimillisiä muistivirheitä ja uudelleenkäyttöä.

Q7: Mikä on raakaan voimaan perustuva hyökkäys?

Hyökkäys, joka testaa järjestelmällisesti jokaisen mahdollisen merkkiyhdistelmän, kunnes oikea salasana löytyy [4].

Q8: Miten tilin lukitus auttaa?

Lukitus tai nopeusrajoitus hidastaa toistuvaa verkossa tehtävää arvausta ja yhdessä valvonnan ja MFA:n kanssa pienentää raakaa voimaa käyttävien hyökkäysten riskiä [4].

Q9: Ovatko pääsalasanat turvallisia?

Ne ovat turvallisia, jos ne ovat korkean entropian salalauseita, joita ei koskaan käytetä uudelleen muissa verkkojärjestelmissä.

Q10: Pitäisikö salasanat vaihtaa säännöllisesti?

NIST:n mukaan määräaikaista vaihtoa ei pidä pakottaa; vaihda salasanat vaarantumisen todisteiden perusteella ja priorisoi pituus, estolistat ja MFA [1].

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

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

Q1: Miten Argon2 vertautuu bcryptiin?

OWASP luettelee Argon2id:n ensisijaiseksi valinnaksi; sen muistiintensiiviset asetukset kestävät GPU- ja ASIC-murtamista paremmin kuin bcrypt [2].

Q2: Mitä on avainvenytys (key stretching)?

Tekniikka, joka toistaa tiivistysalgoritmia tuhansia kertoja salasanan varmennuksen hidastamiseksi ja tekee murtamisesta kallista [2].

Q3: Miten rainbow-taulut toimivat?

Ne ovat esilaskettuja hakutaulukoita, jotka yhdistävät selväkieliset salasanat niiden tiivisteisiin ja joilla suolaamattomat tiivisteet voidaan purkaa nopeasti [2].

Q4: Mitä tunnistetietojen kierrätys on?

Yhdestä tietomurrosta varastettujen käyttäjätunnus-salasanaparien uudelleenkäyttö muihin palveluihin pääsemiseksi erityisesti silloin, kun ihmiset ovat käyttäneet salasanoja uudelleen [3].

Q5: Voivatko salasanojen hallintaohjelmat joutua hakkeroiduiksi?

Kyllä. Monet käyttävät nollatietosalausta (zero-knowledge), joten palvelinmurto paljastaa vain salatut holvit, mutta heikot pääsalasanat voidaan silti murtaa offline-tilassa.

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

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

Q6: Mikä on sanakirjahyökkäys?

Raakaan voimaan perustuva muunnelma, joka testaa yleisiä sanoja, fraaseja ja aiemmin vuodettuja salasanoja satunnaisten kirjainten sijaan.

Q7: Miksi salalauseet ovat parempia?

Salalauseet käyttävät useita satunnaisia sanoja, mikä luo korkean entropian, joka on ihmisen helppo muistaa mutta laskennallisesti kallis murtaa [1].

Q8: Miten kertakirjautuminen (SSO) vaikuttaa salasanavuotoihin?

SSO vähentää salasanojen leviämistä, mutta identiteetintarjoajasta tulee arvokas kohde, joka tarvitsee vahvan, mieluiten tietojenkalastelua kestävän MFA:n [6].

Q9: Mitä istunnon kaappaus on?

Hyökkääjä hankkii tai väärinkäyttää voimassa olevaa istuntotunnusta esiintyäkseen kirjautuneena käyttäjänä tarvitsematta salasanaa uudelleen [5].

Q10: Miten salasanasuihkutus (password spraying) havaitaan?

Etsimällä samoja muutamia salasanoja, joita kokeillaan useilla tileillä, usein hitaasti, jotta jäädään lukitusrajojen alle [7].

Osa 11: 10 tosielämän kyberturvallisuusfaktaa ja havaintoa

Tutustu todellisiin tosiasioihin tietoturvaloukkauksista, puolustusmekanismeista ja vaatimustenmukaisuusstandardeista.

1. TURVALLISUUSOIVALLUS

NIST SP 800-63B edellyttää, että uudet salasanat tarkistetaan yleisten ja vaarantuneiden salasanojen estolistoja vasten [1].

2. TURVALLISUUSOIVALLUS

Vuoden 2019 "Collection #1" -vuoto yhdisti tietoja monista aiemmista tietomurroista yhdeksi valtavaksi sähköposti- ja salasanaparien tiedostoksi [8].

3. TURVALLISUUSOIVALLUS

NIST edellyttää nykyään, että ainoana todennustekijänä käytettävien salasanojen on oltava vähintään 15 merkkiä pitkiä [1].

4. TURVALLISUUSOIVALLUS

ASIC-laitteisto voi laskea miljardeja SHA-256-tiivisteitä sekunnissa, minkä vuoksi raaka SHA-tiivistys ei sovellu käyttäjien salasanoille [2].

5. TURVALLISUUSOIVALLUS

Yksilölliset suolat tarkoittavat, että kaksi käyttäjää, joilla on täsmälleen sama salasana, saavat tietokantaan eri tiivisteet [2].

6. TURVALLISUUSOIVALLUS

Monet salasanahallinnat salaavat holvin tiedot paikallisesti vahvalla salauksella, joka johdetaan käyttäjän pääsalasanasta.

7. TIETOTURVATIETOA

Credential stuffing toimii, koska monet ihmiset käyttävät samaa salasanaa verkkokauppa-, pankki- ja sähköpostitileillä [3].

8. TIETOTURVATIETOA

NIST SP 800-63B:n mukaan tarkistajien ei tule vaatia salasanojen määräajoin vaihtamista, vaan vaihto vaaditaan vasta vaarantumisen todisteiden ilmetessä [1].

9. TIETOTURVATIETOA

Yhden ison kirjaimen ja merkin lisääminen lyhyeen salasanaan ei pysäytä nykyaikaisia automatisoituja GPU-sanakirjahyökkäyksiä [1].

10. TURVALLISUUSOIVALLUS

MFA voi estää monia tunnustentäyttöyrityksiä, vaikka salasana olisi vuotanut; tietojenkalastelua kestävä MFA on vahvempi kuin tekstiviestikoodit [3].

Tekniset viitteet ja lähteet

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

TIETEELLISET JA ALAN VIITTEET

[1] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[2] OWASP. (n.d.). Password Storage Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

[3] OWASP. (n.d.). Credential Stuffing Prevention Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

[4] OWASP. (n.d.). Authentication Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[5] OWASP. (n.d.). Session Management Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[6] CISA. (2022). Implementing Phishing-Resistant MFA (fact sheet).

https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[7] CISA. (2018). Brute Force Attacks Conducted by Cyber Actors (Alert TA18-086A).

https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors

[8] Hunt, T. (2019). The 773 Million Record "Collection #1" Data Breach. Troy Hunt.

https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 **Kysymys 1** — **Oikea vastaus: A**

OPETTAJALLE

Tunnuksentäyttö käyttää automaatiota vuotaneiden käyttäjätunnus–salasana-parien kokeilemiseen muilla sivustoilla [3].

2 **Kysymys 2** — **Oikea vastaus: A**

OPETTAJALLE

OWASP suosittelee ensisijaisesti Argon2id:tä; bcrypt on tarkoitettu lähinnä vanhoille järjestelmille, joissa Argon2id tai scrypt eivät ole käytettävissä [2].

3 **Kysymys 3** — **Oikea vastaus: A**

OPETTAJALLE

MFA vaatii lisätekijän, joten varastettu salasana yksinään ei avaa tiliä [3].

4 **Kysymys 4** — **Oikea vastaus: A**

OPETTAJALLE

Tietomurtojen aineistot ovat vuotaneita tunnuskokoelmia, kuten vuoden 2019 Collection #1 -kokoelma [8].

5 **Kysymys 5** — **Oikea vastaus: A**

OPETTAJALLE

Salasanahallinta luo ja tallentaa ainutlaatuisen, vahvan salasanan jokaiselle tilille, mikä estää uudelleenkäytön [3].

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Kysymys 6** — **Oikea vastaus: Tosi**

OPETTAJALLE

Tosi: uudelleenkäytetyt salasanat antavat hyökkääjien toistaa yhdeltä sivustolta vuotaneita tunnuksia muilla sivustoilla [3].

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

OPETTAJALLE

Epätosi: SHA-1 on nopea tiiviste; OWASP suosittelee sen sijaan Argon2id:tä, scryptiä, bcryptiä tai PBKDF2:ta [2].

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

OPETTAJALLE

Epätosi: monimutkaisuussäännöt yksinään eivät pysäytä tunnuksentäyttöä uudelleenkäytetyillä vuotaneilla salasanoilla; tarvitaan MFA [3].

9 **Kysymys 9** — **Oikea vastaus: Tosi**

OPETTAJALLE

Tosi: valvontapalvelut etsivät tietomurtoaineistoista ja pimeän verkon lähteistä paljastuneita tunnuksia [8].

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

OPETTAJALLE

Tosi: salasanakohtainen ainutlaatuinen suola tekee valmiiksi lasketuista sateenkaaritaulukoista tehottomia [2].

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

F 1. TUNNUSTÄYTTÖ	H 2. BCRYPT	D 3. TIETOMURTO	G 4. SUOLAUS
C 5. HALLINTA	B 6. MFA	A 7. RAINBOW-TAULU	E 8. TIETOJENKALASTELU

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 TÄYTTÖHYÖKKÄYS	2 BCRYPT	3 TIETOMURTO	4 SUOLAUS
5 HALLINNOIJA	6 MFA-TUNNISTUS		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 H – KALASTELU	2 C – TIETOMURTO	3 B – BCRYPT	4 G – RAINBOWTAULU
5 A – TÄYTTÖHYÖKKÄYS	6 D – SUOLAUS	7 E – HALLINNOIJA	8 F – MFATUNNISTUS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit TUNNUSTÄYTTÖ, BCRYPT ja TIETOMURTO omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

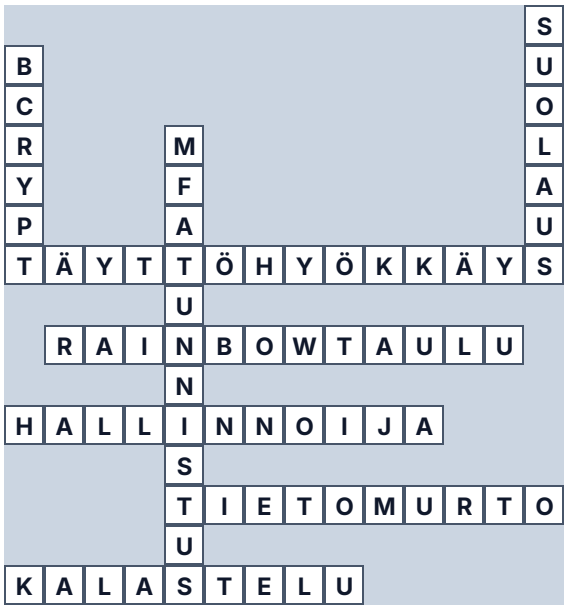
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

4 vaakasuoraan: TÄYTTÖHYÖKKÄYS Vuotaneiden tunnistetietojen testaaminen. (14 kirjainta)

5 vaakasuoraan: RAINBOWTAULU Valmiiksi laskettu salasanatiivisteiden taulukko. (12 kirjainta)

6 vaakasuoraan: HALLINNOIJA Tunnistetietojen tallennustyökalu. (11 kirjainta)

7 vaakasuoraan: TIETOMURTO Tietokannan luvaton paljastuminen. (10 kirjainta)

8 vaakasuoraan: KALASTELU Sosiaalinen manipulointi kirjautumistietojen varastamiseksi. (9 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: SUOLAUS Satunnaisen suolan lisääminen salasanan tiivisteeseen. (7 kirjainta)

2 pystysuoraan: BCRYPT Hidas salasanojen tiivistysalgoritmi. (6 kirjainta)

3 pystysuoraan: MFATUNNISTUS Monivaiheinen kirjautumisen tarkistus. (12 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. KÖYKHYÄÖÄTYSTT — **TÄYTTÖHYÖKKÄYS**
2. TTTIOOURME — **TIETOMURTO**
3. HNNOLAJAIIL — **HALLINNOIJA**
4. LTBIWUOUARAN — **RAINBOWTAULU**
5. YRTBPC — **BCRYPT**
6. UOASLSU — **SUOLAUS**
7. ISUMFNSTUANT — **MFATUNNISTUS**
8. USLKAATEL — **KALASTELU**

SALAKIRJOITUSHAASTEEN AVAIN

"SUOJAA VUOTANEET SALASANAT MFA TUNNISTUKSELLA"

Tapaustutkimusten vastausavain

A Tapaustutkimus 1: Yrityksen käyttötunnusvuodon korjaaminen

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Pimeän verkon valvontapalvelu hälyttää organisaatiota siitä, että yrityksen järjestelmänvalvojien salasanoja sisältävä tietokantavuoto on julkaistu verkossa.
- Suositeltu strategia ja ratkaisu: Peruuta kaikki aktiiviset ylläpitäjien istunnot ja nollaa tunnukset korkean entropian generaattorilla. Pakota tietojenkalastelua kestävä MFA ylläpitoportaaleihin [6], kierrätä vaikutuksen kohteena olevat API-avaimet, tarkista kirjautumislokit, selvitä alkuperäinen altistuminen ja tarkista muut etuoikeutetut tilit.

B Tapaustutkimus 2: Salasanojen tiivistämisstandardien toteuttaminen

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Yrityksen tietokanta tallentaa käyttäjien salasanat vanhentuneilla MD5-tiivisteillä ilman kryptografista suolaa, joten ne ovat alttiita nopealle poimimiselle.
- Suositeltu strategia ja ratkaisu: Ota käyttöön Argon2id (tai bcrypt vanhoissa järjestelmissä) käyttäjäkohtaisella suolalla [2]. Kääri nykyiset MD5-tiivisteet nyt uuteen algoritmiin, tiivistä uudelleen suoraan kunkin käyttäjän seuraavassa kirjautumisessa ja pakota salasanan vaihto pitkään käyttämättömille tileille.