Nafn: _____ Dagsetning: _____ Stig: _____

Vírusvarnarhugbúnaður og endabúnaður Verndarleiðarvísir

Undirskriftargreining, vísindaleg greining (heuristics), atferlisvöktun, einangrun í sandkassa, uppfærslur

NÁMSYFIRLIT UM VÍRUSVARNARHUGBÚNAÐ

VARIÐ
GAGNADULKÓÐUN
256-bita AES staðall

UPPFYLLIR KRÖFUR
ALÞJÓÐLEGIR STAÐLAR
Rammar GDPR og CCPA

ZERO-TRUST
AÐGANGSSTEFNA
Fjölþátta auðkenning

Velkomin! Þetta verkefnahefti leiðir þig í gegnum vírusvarnarhugbúnað og endapunktavernd. Þú munt kynnast undirskriftagagnagrunnum, heuristic-skönnum, hegðunarvöktun, einangruðum sýndarskrám og aðferðum til að draga úr fölskum jákvæðum niðurstöðum.

ÁFANGAR VERKEFNABLAÐSINS

- [ ] **Hluti 1-4: Náðu tökum á netöryggi og varnir gegn ógnum.**
- [ ] **Hluti 5-7: Leystu krossgátur og orðaleitarþrautir.**
- [ ] **Hluti 8-9: Leystu dæmisögur og dulmálsáskorun.**
- [ ] **Hluti 10: Farðu yfir síður með algengum spurningum, grunnstig og framhaldsstig.**
- [ ] **Hluti 11: Kannaðu 10 áhugaverðar staðreyndir úr raunheimum.**
- [ ] **Auka: áskorunin Hugsaðu hratt.**

Opnaðu netöryggisleiðarvísi VPN.com

URL: https://www.vpn.com/is/netoryggd/virusvorn/

Námsvegvísir þinn: vírusvarnarstefna

- Gerðu greinarmun á spilliforritagreiningu sem byggist á undirskriftum og þeirri sem byggist á rökgreiningu (heuristic).
- Skildu hegðunarvöktun og einangrunarreglur sandkassa.
- Metðu áhrif rauntímaskönnunar á afköst kerfis og endapunkta.
- Draga úr röngum jákvæðum flokkunum með staðfestingu stafrænna skírteina.
- Stjórna dreifingu daglegra skilgreiningaruppfærslna á endabúnað fyrirtækis.

LEIÐBEININGAR UM VÍRUSVARNIR

Svaraðu fjölvalsspurningunum og satt/ósatt-spurningunum, kláraðu eyðufyllingarsetningarnar með orðabankanum, paraðu saman skilgreiningar og leystu krossgátuna og orðaleitina. Nýttu þekkingu þína á vírusvarnir fyrir endabúnað. Ljúktu með aukaverkefninu Hugsaðu hratt.

VÍRUSVÖRN OG UNDIRSKRIFTASKÖNNUN (INNGANGUR)

Vírusvarnarhugbúnaður ver endabúnað með því að greina, einangra og fjarlægja spilliforrit. Nútímakerfi sameina undirskriftagagnagrunna (sem passa við þekkt kjötkássagildi ógna) við heuristík (sem greinir uppbyggingu skráa) og atferlisvöktun til að greina núlldagsárásir.

LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT

Áfangi 1: Fjölvalsáskorun

1 **1. Hver eru takmörk greiningar sem byggir á undirskriftum?**

- A. Það getur ekki greint óþekkt eða breytt spilliforrit
- B. Það veldur mörgum fölskum jákvæðum niðurstöðum
- C. Það krefst mikils örgjörvaafls
- D. Það virkar aðeins þegar tengt er við internetið

2 **2. Hvernig finna reynsluskannar ný afbrigði spilliforrita?**

- A. Með því að greina grunsamleg mynstur og kóðauppbyggingu
- B. Með því að bera kjötkássur skráa saman við gagnagrunn yfir ógnir
- C. Með því að eyða sjálfkrafa öllum óundirrituðum keyrsluskrám
- D. Með því að hlaða hverri skrá upp í opna skýjamöppu

3 **3. Hver er tilgangur keyrslu í sandkassa í vírusvörn?**

- A. Að einangra og greina skrár í öruggu sýndarhólfi
- B. Að flýta flutningi afritunar staðbundins skráakerfis
- C. Að uppfæra öryggisplástra staðbundna stýrikerfisins
- D. Að þjappa stórum skjalaskrám til að spara geymslupláss

4 **4. Hvaða greiningaraðferð merkir ógnarhegðun í rauntíma?**

- A. Hegðunargreining sem fylgist með aðgerðum hugbúnaðar
- B. Skoðun á eldri skrám sem framkvæmd er yfir nótt
- C. Notandi þarf sjálfur að tilkynna um hæg forrit
- D. Vikulegar handvirkar yfirferðir uppsettra forrita

5 **5. Hvers vegna eru reglulegar uppfærslur á skilgreiningum mikilvægar fyrir skanna?**

- A. Til að fæða undirskriftarvélar með auðkennum ógna úr gagnagrunni
- B. Til að auka klukkutíðni örgjörva við aðgerðir
- C. Til að breyta skyndiminnistíma DNS-nafnaþjóna á heimsvísu
- D. Til að heimila stillingar fyrir vefkökur í vafra

Áfangi 2: Satt eða ósatt

6 Spurning tf 6

6. Undirskriftargreining ber kjötkássur skráa saman við gagnagrunnslista.

Satt Ósatt

7 Spurning tf 7

7. Reynsluskannar geta gefið falsjákvæðar viðvaranir um örugga skrá.

Satt Ósatt

8 Spurning tf 8

8. Sandkassi leyfir spilliforriti ótakmarkaðan aðgang að netskrám.

Satt Ósatt

9 Spurning tf 9

9. Atferlisskönnun lokar á skrár þegar þær sýna skaðlegar aðgerðir.

Satt Ósatt

10 Spurning tf 10

10. Hefðbundinn vírusvarnarhugbúnaður stöðvar allar núlldagsárásir fullkomlega.

Satt Ósatt

Áfangi 3: Lykilhugtök fyllt inn

Lestu hverja setningu hér að neðan og fylltu í eyðuna með réttu hugtaki úr orðabankanum.

1. Hefðbundinn skanni þekkir spilliforrit með því að bera skrár saman við þekkta _____ .
2. Greining á kóðamynstri skráa kallast skönnun með _____ .
3. Vírusvarnir einangra grunsamlegar skrár í umhverfi sem kallast _____ .
4. Rauntímavöktun fylgist með _____ forrita til að finna grunsamlega virkni.
5. Skannar sækja daglega _____ á gagnagrunni til að þekkja nýjar ógnir.
6. Þegar öruggt forrit er merkt sem spilliforrit kallast viðvörunin _____ .

ORÐABANKI

EINANGRUN HEGÐUN HEURISTÍK RANGJÁKVÆÐ SANDKASSI UNDIRSKRIFT UPPFÆRSLUR VÍRUSVÖRN

Skrifaðu svörin þín hér:

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

Áfangi 4: Pörun hugtaka um öryggi

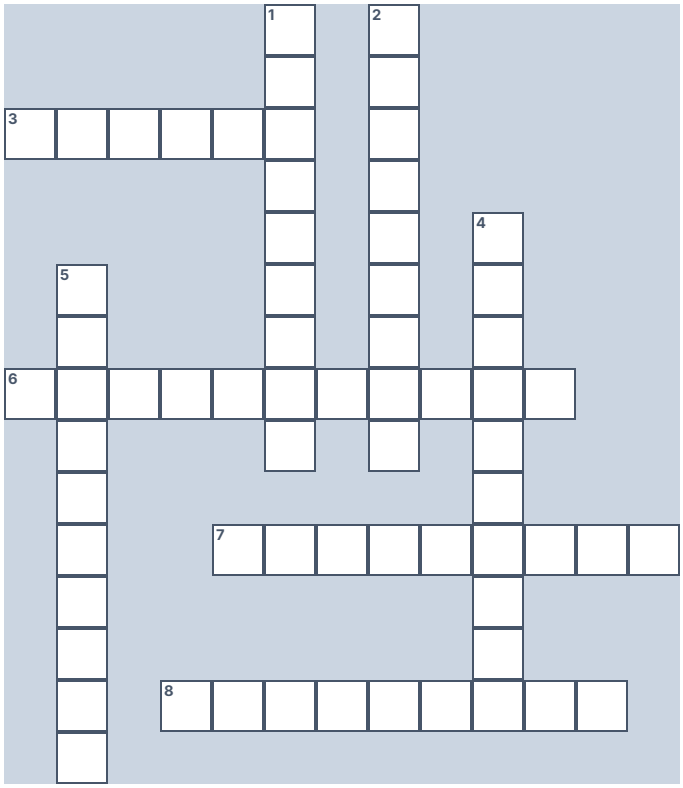
PÖRUN SKILGREININGA

Paraðu hvert hugtak til vinstri við rétta skilgreiningu til hægri með því að skrifa samsvarandi bókstaf (A-H) í útfyllanlega reitinn.

☐	1. Kjötkássaundirskrift	A	Að einangra grunsamlegar skrár til að koma í veg fyrir útsetningu staðbundins kerfis.
☐	2. Heuristísk kóðagreining	B	Hugbúnaðarpakki sem skannar og ver endabúnað gegn veikleikaárásum.
☐	3. Skráarsandkassi	C	Vöktun á aðgerðum hugbúnaðar í keyrslu með tilliti til skaðlegra hegðunarmynstra.
☐	4. Hegðunarskönnun	D	Einkvæmt dulritunarlegt fingrafar í gagnagrunni sem notað er til að bera kennsl á þekktar ógnir.
☐	5. Daglegar uppfærslur	E	Öruggt sýndarprófunarumhverfi sem keyrir óstaðfestan kóða á öruggan hátt.
☐	6. Rangt jákvætt	F	Reglulegt niðurhal skilgreininga sem fæða ógnagagnagrunninn.
☐	7. Einangrun ógna	G	Reglubundin greining sem merkir skrár með grunsamlegri kóðauppbyggingu.
☐	8. Vírusvarnartól	H	Öryggisviðvörun sem flokkar örugg forrit ranglega sem spilliforrit.

Áfangi 5: Krossgáta

Leystu krossgátuna með því að slá stafi inn í virku hvítu reitina. Tölurnar vísa til vísbendinganna hér að neðan.



LÁRÉTT

3. Vöktun á aðgerðum forrita í keyrslu til að finna illgjörn mynstur (6)

6. Einstakt dulritunarlegt fingrafar í gagnagrunni sem notað er til að bera kennsl á þekktar ógnir (11)

7. Reglubundin greining sem merkir skrár með grunsamlegu kóðaskipulagi (9)

8. Grunsamlegar skrár lokaðar af til að koma í veg fyrir að kerfið á tölvunni verði fyrir áhættu (9)

LÓÐRÉTT

1. Öruggt sýndarprófunarumhverfi þar sem ótraustur kóði er keyrður á öruggan hátt (9)

2. Hugbúnaðarpakki sem skannar og ver endabúnað gegn árásum (9)

4. Reglulegt niðurhal skilgreininga sem fæða ógnagagnagrunninn (10)

5. Öryggisviðvörun sem flokkar öruggt forrit ranglega sem spilliforrit (10)

Áfangi 5, valkostur: Aðgengilegar vísbendingar fyrir krossgátu

Notendur skjálesara og lyklaborðs geta slegið svör krossgátunnar beint inn í textareitina hér að neðan. LÁRÉTTAR VÍSBENDINGAR LÓÐRÉTTAR VÍSBENDINGAR

LÁRÉTT

3 lárétt: Vöktun á aðgerðum forrita í keyrslu til að finna illgjörn mynstur (6 stafir):

6 lárétt: Einstakt dulritunarlegt fingrafar í gagnagrunni sem notað er til að bera kennsl á þekktar ógnir (11 stafir):

7 lárétt: Reglubundin greining sem merkir skrár með grunsamlegu kóðaskipulagi (9 stafir):

8 lárétt: Grunsamlegar skrár lokaðar af til að koma í veg fyrir að kerfið á tölvunni verði fyrir áhættu (9 stafir):

LÓÐRÉTT

1 lóðrétt: Öruggt sýndarprófunarumhverfi þar sem ótraustur kóði er keyrður á öruggan hátt (9 stafir):

2 lóðrétt: Hugbúnaðarpakki sem skannar og ver endabúnað gegn árásum (9 stafir):

4 lóðrétt: Reglulegt niðurhal skilgreininga sem fæða ógnagagnagrunninn (10 stafir):

5 lóðrétt: Öryggisviðvörun sem flokkar öruggt forrit ranglega sem spilliforrit (10 stafir):

Áfangi 6: Falið orð í orðaleit

Finndu 8 lykilhugtök sem eru falin í reitnum hér að neðan. Orð geta verið lárétt, lóðrétt eða á ská.

D N Ö Y F J G S Ö Đ N Đ R Ý P
B R V Á A Ö O A Đ K E A Đ O Đ
R Ö É G I Đ S N R M I E I T Ö
U V U É R X É D A A N R Ó N P
L S Ú Þ R U J K S Ú A T D R N
S U Æ B F N T A Ý Y N Í A A S
R R Ö Æ Æ D K S H F G I M N S
Æ Í J L L I U S E Ó R G P G R
F V G Ö A R O I U X U F V J B
P Æ T Æ Á S G L R Ö N G N Á J
P O P N Ý K B L I Ö Æ F U K Þ
U Ó Y V K R V P S Á O X Đ V Ú
L G X D Þ I V J T S Á Ý G Æ Ö
Þ M T R Ý F I Ó Í Đ A D E Đ J
R Y Ý Ý K T Í H K Ú H F H Á É

ORÐALISTI

UNDIRSKRIFT
HEURISTÍK
SANDKASSI
EINANGRUN
HEGÐUN
VÍRUSVÖRN
UPPFÆRSLUR
RANGJÁKVÆÐ

Áfangi 6, valkostur: Aðgengileg orðaforðapörun

Paraðu hvert af hugtökunum 8 úr orðaleitinni við rétta skilgreiningu með því að skrifa bókstafinn (A-H) í eyðuna.

HUGTÖK

A. UNDIRSKRIFT

B. HEURISTÍK

C. SANDKASSI

D. HEGÐUN

E. UPPFÆRSLUR

F. RANGJÁKVÆÐ

G. EINANGRUN

H. VÍRUSVÖRN

SKILGREININGAR OG PÖRUNARREITIR

1. Vöktun á aðgerðum forrita í keyrslu til að finna illgjörn mynstur.
2. Hugbúnaðarpakki sem skannar og ver endabúnað gegn árásum.
3. Reglulegt niðurhal skilgreininga sem fæða ógnagagnagrunninn.
4. Reglubundin greining sem merkir skrár með grunsamlegu kóðaskipulagi.
5. Grunsamlegar skrár lokaðar af til að koma í veg fyrir að kerfið á tölvunni verði fyrir áhættu.
6. Einstakt dulritunarlegt fingrafar í gagnagrunni sem notað er til að bera kennsl á þekktar ógnir.
7. Öruggt sýndarprófunarumhverfi þar sem ótraustur kóði er keyrður á öruggan hátt.
8. Öryggisviðvörun sem flokkar öruggt forrit ranglega sem spilliforrit.

Áfangi 7: Áskorun með ruglaðum orðum

Raðaðu stöfunum hér að neðan í rétta röð til að afhjúpa lykilhugtök um netöryggi. Skrifaðu svörin þín í reitina sem fylgja.

1. **RKFNSRUIDTI** _____
2. **ISSDAASKN** _____
3. **URUSPÆRFLP** _____
4. **NNUARGEIN** _____
5. **TIEKSRHÍU** _____
6. **UÐHGNE** _____
7. **AGRKÁVÆÐJN** _____
8. **NSRVUÍVÖR** _____

Aukaverkefni: Hugsaðu hratt

3 SVÖR Í HVERJUM FLOKKI. SÁ VINNUR SEM FYLLIR FYRST ÚT LISTANN.

1	Ástæður fyrir því að uppfæra hugbúnað			
2	Fólk sem þú getur leitað til varðandi upplýsingatæknihjálp			
3	Hlutir til að gera þegar vírusvörn finnur eitthvað			
4	Merki um tölvuvírus			
5	Hlutir sem eru settir í sóttkví			
6	Staðir þar sem vírusar leynast			
7	Upplýsingar sem þú ættir aldrei að deila			
8	Tegundir skaðlegs hugbúnaðar			
9	Öryggisverkfæri sem þú þekkir			
10	Hlutir sem vírusvörn skannar			
11	Hlutir sem þú afritar			
12	Tæki sem hægt er að brjótast inn í			
13	Vírusvarnarforrit sem þú þekkir			
14	Ástæður fyrir fölskum viðvörunum			
15	Öruggar venjur sem þú getur byrjað á í dag			

Áfangi 8: Dæmisögur um netöryggi

Nýttu hugtökin sem þú hefur lært til að leysa raunveruleg dæmi hér að neðan.

DÆMISAGA 1: SKÖNNUN MEÐ UNDIRSKRIFTUM Í SAMANBURÐI VIÐ HEURISTÍSKA

👨‍💻

Aðstæður: Starfsmaður sækir sérsmíðað tól sem annað teymi smíðaði innanhúss. Undirskriftaskanninn hleypir því í gegn, en vísindalegi skanninn merkir það sem grunsamlegt.

Umræðuspurning: Útskýrðu hvers vegna þetta gerðist og hvernig hægt er að sannreyna hvort skráin sé örugg.

DÆMISAGA 2: MEÐHÖNDLUN RANGRA JÁKVÆÐRA NIÐURSTAÐNA

👨‍💻

Aðstæður: Hugbúnaðarframleiðandi þýðir forritið sitt. Vírusvörn kerfisins merkir nýju keyrsluskrána sem spilliforrit og setur hana í sóttkví.

Umræðuspurning: Gerðu grein fyrir áhættunni af undanþágulistum og lýstu réttri lausnarleið.

Áfangi 9: Leystu dulmálið

Netöryggissérfræðingur ver netkerfiseignir gegn ógnaraðilum á netinu. Notaðu lykilinn „bókstafur í tölu“ hér að neðan til að afkóða skilaboðin með því að skrifa samsvarandi bókstafi í auðu reitina.

DULMÁLSLYKILL: STAFIR Í TÖLUR

A=1 Á=2 B=3 C=4 D=5 Đ=6 E=7 É=8 F=9 G=10 H=11 I=12

Í=13 J=14 K=15 L=16 M=17 N=18 O=19 Ó=20 P=21 Q=22 R=23 S=24

T=25 U=26 Ú=27 V=28 W=29 X=30 Y=31 Ý=32 Z=33 Þ=34 Æ=35 Ö=36

9	12	18	18	5	26		18	32

24	21	12	16	16	12	9	19	23	23	12	25		17	7	6

11	7	26	23	12	24	25	13	15

Afkóðuð skilaboð:

ÁBENDING: HVER TALA STENDUR FYRIR STÖÐU STAFSINS Í STAFRÓFINU (T.D. 1 = A, 2 = B, 36 = Ö).

Áfangi 10: Algengar spurningar um netöryggi – grunnstig (Hluti A)

Farðu yfir algengar spurningar og svör um varnir gegn netógnum.

Q1: Hvernig greinir vírusvarnarhugbúnaður spilliforrit?

Það greinir spilliforrit með samanburði við undirskriftir í gagnagrunni, reynslugreiningu á kóðauppbyggingu og rauntímavöktun á hegðun.

Q2: Hvað er greining byggð á undirskriftum?

Það er skönnunaraðferð sem ber saman dulritunartætigildi skráa við gagnagrunnslista yfir þekktar spilliforritaógnir.

Q3: Hvað er atferlisgreinandi skanni (heuristic scanner)?

Reynsluleit greinir uppbyggingu skráar og kóðaskipanir og merkir grunsamleg mynstur sem eru algeng í afbrigðum spilliforrita.

Q4: Hvað þýðir það þegar skrá er sett í sóttkví?

Vírusvörnin flytur skrána í öruggt, einangrað sóttkvíarsvæði og kemur í veg fyrir keyrslu hennar til að vernda stýrikerfið.

Q5: Hvað er fölsk jákvæð niðurstaða í vírusvörn?

Það er villa þar sem lögmætur, öruggur hugbúnaður er ranglega merktur sem spilliforrit af skönnunarreikniritum.

Áfangi 10: Algengar spurningar um netöryggi – grunnstig (Hluti B)

Farðu yfir algengar spurningar og svör um varnir gegn netógnum.

Q6: Hvernig ver atferlisvöktun kerfi?

Það vaktar hugbúnað sem er í gangi í rauntíma og lokar á ferli sem reyna grunsamlegar breytingar eins og innsetningu kóða.

Q7: Hvers vegna er sandkassaprófun mikilvæg?

Sandkassakeyrsla keyrir óáreiðanlegar skrár í einangraðri sýndarvél og fylgist örugglega með aðgerðum án þess að kerfið berskjaldist.

Q8: Hversu oft ætti að uppfæra vírusskilgreiningar?

Skannar ættu að uppfæra skilgreiningar daglega eða á klukkustundar fresti til að þekkja nýuppgötvuð afbrigði spilliforrita.

Q9: Hver er munurinn á vírusvörn og EDR?

Vírusvörn beinist að skráaskönnun en Endpoint Detection and Response (EDR) veitir ógnarrakningu og einangrun á öllu netinu.

Q10: Get ég keyrt tvö vírusvarnarforrit saman?

Nei. Tveir virkir skannar valda árekstrum í kerfinu, hægja á afköstum og geta hindrað aðgerðir hvor annars.

Áfangi 10: Algengar spurningar um öryggi – framhaldsstig (Hluti C)

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q1: Hvernig draga rökgreiningarreglur (heuristic) úr því að ógnir komist framhjá?

Reynsluleit greinir almenn ógnarmynstur frekar en tilteknar undirskriftir og nær þannig breyttum afbrigðum þekktra spilliforritaætta.

Q2: Hvað er fjölbreytileg veira (polymorphic virus)?

Það er spilliforrit sem breytir skráaruppbyggingu sinni og afkóðunarrútínu við hverja keyrslu, sem gerir undirskriftarskönnun gagnslausa.

Q3: Hvernig greina sandkassar tilraunir til að sniðganga sýndarvélar?

Nútíma sandkassar herma eftir músarsmellum og keyrslutíma kerfis og blekkja spilliforrit sem er hannað til að fela sig þegar það keyrir í sýndarvélum.

Q4: Hvaða niðurhalssnið eru fyrir uppfærslur undirskrifta?

Uppfærslur eru yfirleitt léttar stigvaxandi tvíundarmismunarskrár, sem lágmarka bandbreiddarnotkun biðlarans.

Q5: Hvernig stýra endabúnaðarforrit staðbundnum skönnunum?

Umboðsforrit framkvæma léttar bakgrunnsathuganir og færa djúpar uppflettingar á dulritunarhakkgildum yfir í ógnargagnagrunna í skýinu.

Áfangi 10: Algengar spurningar um öryggi – framhaldsstig (Hluti D)

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q6: Hvað er skönnun fyrir rótarsett (rootkit)?

Það skannar minnistöflur á kjarnastigi og sneiðir hjá API stýrikerfisins sem rótarbúnaður (rootkits) hakar í til að fela virka þræði sína.

Q7: Hvernig lokar atferlisskönnun á gíslatökuforrit?

Það greinir sjálfvirkar lykkjur fjöldadulkóðunar skráa og stöðvar hýsilferlið áður en kerfisgagnagrunnum er læst.

Q8: Hvað er sannprófun á undirritunarskírteini kóða?

Skannar bera stafrænar undirskriftir kóða saman við traust rótarvottunaraðila og sannreyna þannig auðkenni hugbúnaðarframleiðandans.

Q9: Hvernig hafa pökkunarforrit (packers) áhrif á skönnunarvélar?

Pökkunarforrit þjappa eða dulkóða farm spilliforrits. Skannar verða að afpakka skrána í minni áður en leitað er að samsvörun við undirskriftir.

Q10: Hvernig gera EDR-tól einangrun sjálfvirka?

EDR-umboð setja sýkta endapunkta í sóttkví á netstigi, sem hindrar hliðarhreyfingu en leyfir greinendum aðgang.

Hluti 11: 10 staðreyndir um netöryggi og innsýn úr raunheimum

Farðu yfir raunverulegar staðreyndir um öryggisbrot, varnarkerfi og reglufylgnistaðla.

1. INNSÝN Í ÖRYGGI

Undirskriftagagnagrunnar geyma kjötkássur þekktra spilliforrita, svo glæný eða breytt skrá fer fram hjá þeim þar til skilgreiningar eru uppfærðar.

2. INNSÝN Í ÖRYGGI

Reynsluleitarvélar geta merkt sum ný afbrigði spilliforrita áður en undirskriftir eru til, á kostnað fleiri falsjákvæðra niðurstaðna.

3. INNSÝN Í ÖRYGGI

Falskar jákvæðar viðvaranir kosta upplýsingatækniteymi tíma sem fer í að sannreyna og endurheimta skrár sem ranglega voru settar í sóttkví.

4. INNSÝN Í ÖRYGGI

Fjölbreytilegt spilliforrit (polymorphic malware) breytir kóða sínum með hverju afriti, svo varnaraðilar sameina undirskriftir við rökgreiningu og atferlisathuganir.

6. INNSÝN Í ÖRYGGI

Höfundar spilliforrita skrifa sérsniðinn kóða sem athugar sandkassaumhverfi og seinkar keyrslu til að sneiða hjá tímamælum.

5. INNSÝN Í ÖRYGGI

Skýjabyggðar veiruvarnarvélar bera tætigildi grunsamlegra skráa saman við stóra netgagnagrunna um ógnir nánast í rauntíma.

7. ÖRYGGISINNSÝN

Söluaðilar senda reglulega skilgreiningaruppfærslur til endapunkta svo skannar geti greint nýlega staðfestar ógnir.

8. ÖRYGGISINNSÝN

Atferlisvöktun gegn gíslatökuforritum beinist að tilteknum Win32 API-köllum sem tengjast dulkóðun skráa og eyðingu skuggaafrita.

9. ÖRYGGISINNSÝN

Gildar kóðaundirskriftir geta dregið úr hættu á fölskum jákvæðum niðurstöðum, en undirritaðar skrár eru samt skannaðar, þar sem spilliforrit getur líka verið undirritað.

10. INNSÝN Í ÖRYGGI

Rótarsett breyta kerfisgerðum kjarnans og krefjast sérhæfðra skanna við ræsingu til að finna og hreinsa.

Tæknilegar heimildir og tilvísanir

Námsleiðbeiningarnar og gagnvirku þrautirnar eru unnar úr alþjóðlegum stöðlum NIST og OWASP og kröfum um persónuverndarsamræmi. FRÆÐILEGAR HEIMILDIR OG HEIMILDIR ÚR ATVINNUGREININNI

FRÆÐILEGAR HEIMILDIR OG HEIMILDIR ÚR ATVINNUGREININNI

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

https://csrc.nist.gov/pubs/sp/800/83/r1/final

[2] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[3] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[4] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[5] 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

Lausnir: Áfangi 1 – Fjölval

1 **Spurning 1** UNDIRSKRIFTIR Rétt svar: A

ATHUGASEMD FYRIR KENNARA

Undirskriftarskönnun byggir á þekktum tætigildum í gagnagrunni og nær því ekki að greina óþekkt eða breytt spilliforrit. Heimild: OWASP Secure Configuration.

2 **Spurning 2** REYNSLUREGLUR Rétt svar: A

ATHUGASEMD FYRIR KENNARA

Heuristík greinir uppbyggingu kóða og skipanir til að finna grunsamleg einkenni nýrra afbrigða ógna. Heimild: Center for Internet Security (CIS).

3 **Spurning 3** SANDKASSAKEYRSLA Rétt svar: A

ATHUGASEMD FYRIR KENNARA

Sandkassi keyrir grunsamlegar skrár í einangraðri sýndarvél til að fylgjast örugglega með hegðun við keyrslu. Heimild: NIST Digital Identity.

4 **Spurning 4** ATFERLIS- Rétt svar: A

ATHUGASEMD FYRIR KENNARA

Hegðunarskönnun fylgist með forritum í keyrslu í rauntíma til að loka á óleyfilegar kerfisbreytingar. Heimild: Center for Internet Security (CIS).

5 **Spurning 5** UPPFÆRSLUR Rétt svar: A

ATHUGASEMD FYRIR KENNARA

Skannar sækja daglegar stigvaxandi skilgreiningaruppfærslur til að vera í takt við ógnalandslagið. Heimild: OWASP Secure Configuration.

Lausnir: Áfangi 2 – Satt eða ósatt

6 **Spurning 6** UNDIRSKRIFTIR **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Undirskriftartól reikna dulritunartætigildi og bera þau saman við gagnagrunn yfir þekkt tætigildi ógna. Heimild: OWASP Secure Configuration.

7 **Spurning 7** REYNSLUREGLUR **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Heuristískar vélar keyra reglubundna greiningu sem getur merkt lögmætar og öruggar skrár sem grunsamlegar. Heimild: Center for Internet Security (CIS).

8 **Spurning 8** SANDKASSAKEYRSLA **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Sandkassi keyrir kóða í sýndargámi og lokar stranglega á aðgang að netdeilingum. Heimild: NIST Digital Identity.

9 **Spurning 9** ATFERLIS- **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Rauntímavöktun merkir ferli í keyrslu sem reyna ólöglegar skrifaðgerðir eða skráalæsingu. Heimild: Center for Internet Security (CIS).

10 **Spurning 10** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Engin vírusvörn stöðvar allar núlldagsárásir; óþekktar ógnir geta komist framhjá undirskriftum og vísindalegri greiningu.

Orðalyklar og matskvarði

Einkunnaviðmið kennara: Gefðu 1 stig fyrir hverja rétta pörun (alls 8 stig) og hvert samhengishugtak (alls 6 stig).

ÁFANGI 4: LAUSNIR – PÖRUN HUGTAKA

D 1. Kjötkássaundirskrift	G 2. Heuristísk kóðagreining	E 3. Skráarsandkassi	C 4. Hegðunarskönnun
F 5. Daglegar uppfærslur	H 6. Rangt jákvætt	A 7. Einangrun ógna	B 8. Vírusvarnartól

ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

1 UNDIRSKRIFT	2 HEURISTÍK	3 SANDKASSI	4 HEGÐUN
5 UPPFÆRSLUR	6 RANGJÁKVÆÐ		

ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

1 D – HEGÐUN	2 H – VÍRUSVÖRN	3 E – UPPFÆRSLUR	4 B – HEURISTÍK
5 G – EINANGRUN	6 A – UNDIRSKRIFT	7 C – SANDKASSI	8 F – RANGJÁKVÆÐ

UMRÆÐUATRIÐI FYRIR KENNARA

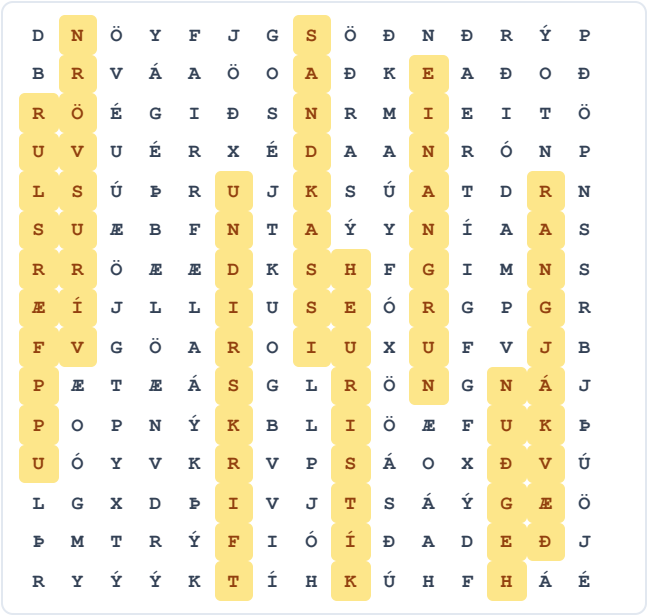
Lykilhugtök:
Athugaðu hvort nemendur geti útskýrt Kjötkássaundirskrift, Heuristísk kóðagreining og Skráarsandkassi með eigin orðum og gefið dæmi um hvert hugtak.

Dæmisögur:
Biddu nemendur að styðja tillögur sínar með staðreyndum úr verkefnablaðinu en ekki ágiskunum.

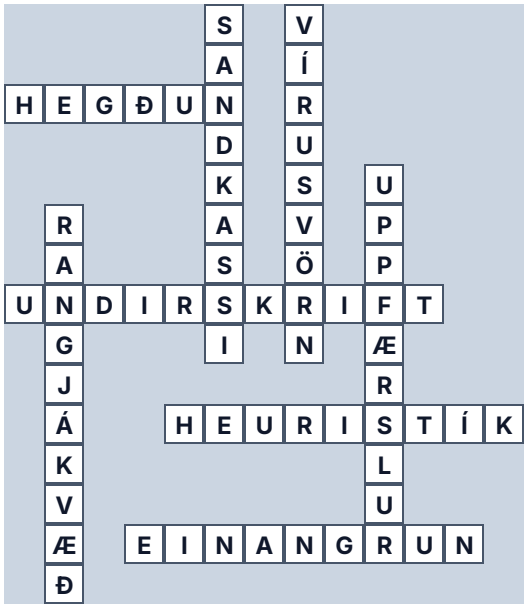
Mat á heimildum:
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

Lausnir við þrautum og athugasemdir fyrir kennara

LAUSN ORÐALEITAR



LAUSN KROSSGÁTUNNAR



LÁRÉTT

3 lárétt: HEGÐUN Vöktun á aðgerðum forrita í keyrslu til að finna illgjörn mynstur (6 stafir)

6 lárétt: UNDIRSKRIFT Einstakt dulritunarlegt fingrafar í gagnagrunni sem notað er til að bera kennsl á þekktar ógnir (11 stafir)

7 lárétt: HEURISTÍK Reglubundin greining sem merkir skrár með grunsamlegu kóðaskipulagi (9 stafir)

8 lárétt: EINANGRUN Grunsamlegar skrár lokaðar af til að koma í veg fyrir að kerfið á tölvunni verði fyrir áhættu (9 stafir)

LÓÐRÉTT

1 lóðrétt: SANDKASSI Öruggt sýndarprófunarumhverfi þar sem ótraustur kóði er keyrður á öruggan hátt (9 stafir)

2 lóðrétt: VÍRUSVÖRN Hugbúnaðarpakki sem skannar og ver endabúnað gegn árásum (9 stafir)

4 lóðrétt: UPPFÆRSLUR Reglulegt niðurhal skilgreininga sem fæða ógnagagnagrunninn (10 stafir)

5 lóðrétt: RANGJÁKVÆÐ Öryggisviðvörun sem flokkar öruggt forrit ranglega sem spilliforrit (10 stafir)

Lausnir: Stafaruglingur og dulmál

Lausnalykill fyrir virkni um að raða orðaforða og Secret Cipher Challenge.

LYKILL ORÐARAÐAR

1. R K F N S R U I D T I — **UNDIRSKRIFT**
2. I S S D A A S K N — **SANDKASSI**
3. U R U S P Æ R F L P — **UPPFÆRSLUR**
4. N N U A R G E I N — **EINANGRUN**
5. T I E K S R H Í U — **HEURISTÍK**
6. U Ð H G N E — **HEGÐUN**
7. A G R K Á V Æ Ð J N — **RANGJÁKVÆÐ**
8. N S R V U Í V Ö R — **VÍRUSVÖRN**

LYKILL AÐ LEYNIDULMÁLSÞRAUT

"FINNDU NÝ SPILLIFORRIT MEÐ HEURISTÍK"

Lausnir dæmisagna

A Dæmisaga 1: Skönnun með undirskriftum í samanburði við heuristíska

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Greining aðstæðna: Starfsmaður sækir sérsmíðað tól sem annað teymi smíðaði innanhúss. Undirskriftarskanninn hleypir því í gegn en mynsturskanninn merkir það sem grunsamlegt.
- Ráðlögð aðferð og lausn: Hvers vegna það gerðist: Undirskriftarskönnun athugar skráarhakk; þar sem skráin er sérsmíðuð er hún ekki í ógnagagnagrunninum. Mynsturgreining skoðar uppbyggingu og merkti grunsamlegar aðgerðir (t.d. skrifun í skrásetningu). Staðfesting: Keyrðu skrána í sandkassa til að fylgjast með aðgerðum, athugaðu stafrænar undirskriftir og sendu hakkið á ógnargreindargáttir.

B Dæmisaga 2: Meðhöndlun rangra jákvæðra niðurstaðna

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Greining aðstæðna: Hugbúnaðarframleiðandi þýðir forritið sitt. Vírusvörn kerfisins merkir nýju keyrsluskrána sem spilliforrit og setur hana í sóttkví.
- Ráðlögð aðferð og lausn: Hættur við undanþágur: Að sniðganga skannara getur leyft raunverulegum, sýktum kóða að keyra. Leið til lausnar: Sendu skrána til vírusvarnarframleiðandans til greiningar, undirritaðu kóðann stafrænt með vottunaraðilum og stilltu tímabundið undanþágur fyrir tilteknar möppur í stað þess að slökkva á vírusvörninni.