Ainm: _____ **Dáta:** _____ **Scór:** _____

Bogearraí frithvíris agus críochphointe Treoir Chosanta

Brath sínithe, heoiristící, monatóireacht iompair, bosca gainimh, nuashonruithe

ACHOIMRE FOGHLAMA AR BHOGEARRAÍ FRITHVÍRIS

SLÁNAITHE

CRIPTIÚ SONRAÍ

Caighdeán AES 256-giotán

COMHLÍONTACH

CAIGHDEÁIN DHOMHANDA

Creataí GDPR agus CCPA

IONTAOBHAS NIALASACH

POLASAÍ ROCHTANA

Fíordheimhniú ilfhachtóra

Fáilte! Treoraíonn an paca gníomhaíochtaí seo thú trí bhogearraí frithvíris agus cosaint chríochphointe. Déanfaidh tú iniúchadh ar bhunachair shonraí sínithe, scanóirí heorastúla, monatóireacht iompair, comhaid fhíorúla bosca gainimh, agus maolú dearbhuithe bréagacha.

SEICPHOINTÍ NA BILEOGE OIBRE

- [ ] **Cuid 1-4: Máistrigh cibearshlándáil agus cosc bagairtí.**
- [ ] **Cuid 5-7: Réitigh tras-fhocail agus puzail cuardaigh focal.**
- [ ] **Cuid 8-9: Réitigh cás-staidéir agus dúshlán cód.**
- [ ] **Cuid 10: Déan athbhreithniú ar leathanaigh Ceisteanna Coitianta bunúsacha agus ardleibhéil.**
- [ ] **Cuid 11: Féach ar 10 bhfíric spéisiúla ón domhan fíor.**
- [ ] **Breis: dúshlán Smaoinigh go tapa.**

Oscail Treoir VPN.com ar Chibearshlándáil

URL: https://www.vpn.com/ga/slandail-dhigiteach/frithvireas/

Do threoirmhapa foghlama: straitéis frithvíris

- Idirdhealaigh idir brath bogearraí mailíseacha bunaithe ar shínithe agus brath bunaithe ar heoirisic.
- Tuig monatóireacht iompair agus prótacail scoite bosca gainimh.
- Meas tionchair scanta fíor-ama ar fheidhmíocht an chórais agus ar chríochphointí.
- Aicmithe bréagdhearfacha a mhaolú trí fhíorú teastas digiteach.
- Bainistigh dáileadh nuashonruithe sainmhínithe laethúla ar chríochphointí corparáideacha.

TREOIRLÍNTE TREOIR FRITHVÍRIS

Freagair na ceisteanna ilrogha agus fíor/bréagach, comhlánaigh na habairtí le bearnaí leis an mbanc focal, meaitseáil sainmhínithe, agus réitigh an crosfhocal agus an cuardach focal. Cuir do chuid eolais i bhfeidhm ar shlándáil frithvíreas críochphointe. Críochnaigh leis an ngníomhaíocht bhreise Smaoinigh go tapa.

COSAINT FRITHVÍRIS AGUS SCANADH SÍNITHE (RÉAMHRÁ)

Cosnaíonn bogearraí frithvíris críochphointe trí bhogearraí mailíseacha a aithint, a chur i gcoraintín agus a bhaint. Comhcheanglaíonn córais nua-aimseartha bunachair shínithe (a mheaitseálann haiseanna bagairtí aitheanta) le heuristicí (a anailísíonn struchtúr comhaid) agus monatóireacht iompair chun saothruithe lae nialais a bhrath.

LÉIGH GACH SEICPHOINTE GO CÚRAMACH AGUS ROGHNAIGH NÓ SCRÍOBH AN FREAGRA CEART

Seicphointe 1: Dúshlán ilrogha

1. **1. Cad é teorainn na braite bunaithe ar shínithe?**
   - A. Ní féidir leis bogearraí mailíseacha anaithnide nó modhnaithe a aithint
   - B. Gineann sé ráta ard dearfach bréagach
   - C. Éilíonn sé cumhacht phróiseála ard CPU
   - D. Oibríonn sé nuair a bhíonn sé ceangailte leis an idirlíon amháin

2. **2. Conas a bhraitheann scanóirí eurasacha leaganacha nua bogearraí mailíseacha?**
   - A. Trí phatrúin agus struchtúir chóid amhrasacha a aithint
   - B. Trí hashanna comhad a mheaitseáil le bunachar sonraí bagairtí
   - C. Trí gach inrite gan síniú a scriosadh go huathoibríoch
   - D. Trí gach comhad a uaslódáil chuig fillteán scamall poiblí

3. **3. Cad é cuspóir fhorghníomhú bosca gainimh an fhrithvíris?**
   - A. Comhaid a leithlisiú agus a anailísiú i gcromán fíorúil slán
   - B. Aistriú cúltaca córais comhad áitiúil a luasghéarú
   - C. Paistí slándála an chórais oibriúcháin áitiúil a nuashonrú
   - D. Comhaid mhóra doiciméad a chomhbhrú chun stóras a shábháil

4. **4. Cén modh braite a chuireann bratach ar iompar bagartha i bhfíor-am?**
   - A. Anailís iompraíochta a dhéanann monatóireacht ar ghníomhartha bogearraí
   - B. Iniúchadh ar logaí stairiúla a dhéantar thar oíche
   - C. Idirghabháil láimhe ón úsáideoir ag tuairisciú feidhmchlár mall
   - D. Athbhreithnithe seachtainiúla láimhe ar chláir shuiteáilte

5. **5. Cén fáth a bhfuil nuashonruithe rialta sainmhínithe ríthábhachtach do scanóirí?**
   - A. Aitheantóirí bagartha bunachair sonraí inneall sínithe a bheathú
   - B. Luasanna clog LAP a mhéadú le linn oibríochtaí
   - C. Chun amanna taiscthe freastalaí ainmneacha DNS domhanda a athrú
   - D. Socruithe fianán an bhrabhsálaí gréasáin a údarú

Seicphointe 2: Dúshlán Fíor nó Bréagach

6 **Ceist F/B 6**

6. Meaitseálann brath sínithe hais chripteagrafacha comhad le liostaí bunachair sonraí.

○ Fíor ○ Bréagach

7 **Ceist F/B 7**

7. Is féidir le scanóirí eurasacha foláirimh dhearfacha bhréagacha a spreagadh ar chomhaid shábháilte.

○ Fíor ○ Bréagach

8 **Ceist F/B 8**

8. Ligeann bosca gainimh do bhogearraí mailíseacha rochtain a fháil ar chomhaid líonra gan teorainn.

○ Fíor ○ Bréagach

9 **Ceist F/B 9**

9. Blocálann scanadh iompair comhaid nuair a thaispeánann siad gníomhartha mailíseacha.

○ Fíor ○ Bréagach

10 **Ceist F/B 10**

10. Stopann bogearraí antaivíris caighdeánacha gach ionsaí zero-day go hiomlán.

○ Fíor ○ Bréagach

Seicphointe 3: Príomhthéarmaí a chur isteach

Léigh gach abairt thíos agus líon isteach an bhearna leis an téarma ceart ón mBanc Focal.

1. Déanann scanóir traidisiúnta meaitseáil le _____ chun bogearraí mailíseacha aitheanta a aithint.

2. Tugtar scanadh _____ ar anailís a dhéanamh ar phatrúin chód comhaid.

3. Cuireann uirlisí frithvíris comhaid amhrasacha ar leith i dtimpeallacht ar a dtugtar _____ .

4. Coimeádann monatóireacht fíor-ama súil ar _____ na gclár le haghaidh gníomhaíochtaí amhrasacha.

5. Íoslódálann scanóirí _____ ar an mbunachar sonraí gach lá chun bagairtí nua a aithint.

6. Nuair a mharcáiltear cláir shábháilte mar bhogearraí mailíseacha, is _____ an rabhadh a eascraíonn.

BANC FOCAL FOCLÓIRE

BOSCA GAINIMH BRÉAGDHEARFACH CUARANTÍN FRITHVÍREAS HEORASTAIC IOMPAR NUASHONRUITHE SÍNIÚ HAISISE

Scríobh do fhreagraí anseo:

1. **2.**

3. **4.**

5. **6.**

Seicphointe 4: Meaitseáil coincheapa slándála

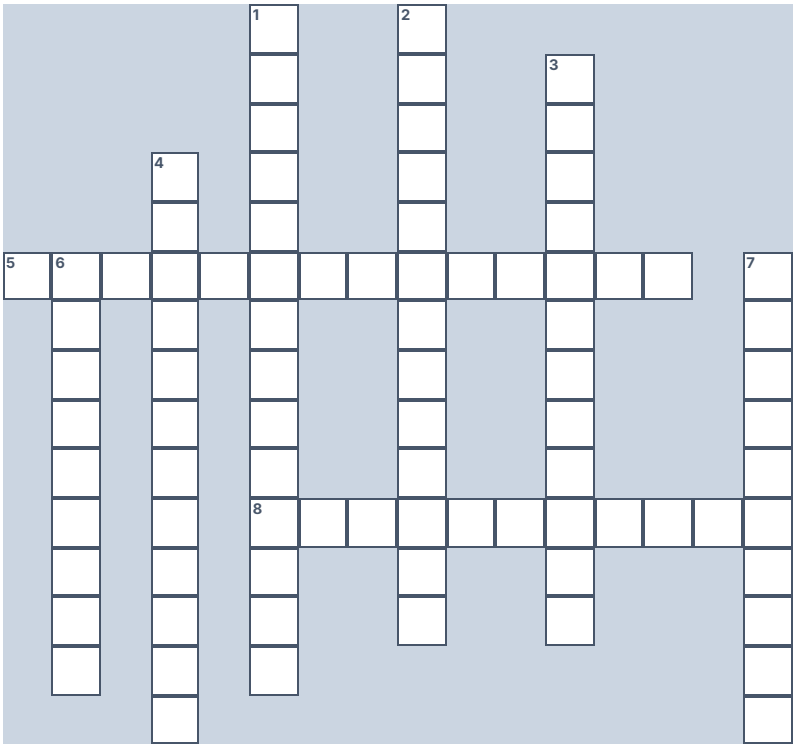
MEAITSEÁIL SAINMHÍNITHE

Meaitseáil gach téarma foclóra ar chlé lena shainmhíniú ceart ar dheis trí scríobh na litreach comhfhreagraí (A-H) sa bhosca ionchuir inlíonta.

	1. Síniú haise	A	Comhaid amhrasacha a theorannú chun nochtadh an chórais áitiúil a chosc.
	2. Heoiristící cóid	B	Sraith bogearraí a scanann agus a chosnaíonn cinn scríbe ó shaothrú.
	3. Bosca gainimh comhaid	C	Monatóireacht ar ghníomhartha bogearraí reatha le haghaidh patrúin oibríochta mailíseacha.
	4. Scanadh iompair	D	Lorg uathúil bunachair sonraí chripteagrafach a úsáidtear chun bagairtí aitheanta a aithint.
	5. Nuashonruithe laethúla	E	Timpeallacht tástála fhíorúil shlán a rithfeas cód neamhiontaofa go sábháilte.
	6. Dearfach bréagach	F	Íoslódálacha rialta sainmhínithe a chothaíonn bunachar sonraí na mbagairtí.
	7. Leithlisiú bagairtí	G	Anailís bunaithe ar rialacha a mharcálann comhaid a bhfuil leaganacha cóid amhrasacha acu.
	8. Uirlis frithvíreas	H	Rabhadh slándála a rangaíonn bogearraí sábháilte mar bhogearraí mailíseacha go mícheart.

Seicphointe 5: Crosfhocal

Réitigh an crosfhocal trí litreacha a chlóscríobh sna boscaí bána gníomhacha. Freagraíonn na huimhreacha do na leideanna thíos.



TRASNA

5. Monatóireacht ar ghníomhartha bogearraí atá ag rith le haghaidh patrúin oibríochta mailíseacha. (14)

8. Sraith bogearraí a scanann agus a chosnaíonn críochphointí ó bhrattaí leochaileachta. (11)

SÍOS

1. Rabhadh slándála a aicmíonn bogearraí sábháilte go mícheart mar bhogearraí mailíseacha. (14)

2. Íoslódálacha rialta sainmhínithe a chothaíonn bunachar sonraí na mbagairtí. (13)

3. Timpeallacht fhíorúil thástála shlán ina ritear cód nach bhfuil iontaofa go sábháilte. (12)

4. Lorg uathúil chripteagrafach bunachair a úsáidtear chun bagairtí aitheanta a aithint. (12)

6. Comhaid amhrasacha a theorannú chun nochtadh an chórais áitiúil a sheachaint. (9)

7. Anailís rialachbhunaithe a chuireann comhaid le leaganacha amhrasacha cóid in iúl. (10)

Seicphointe 5, rogha eile: Leideanna crosfhocail inrochtana

Is féidir le húsáideoirí léitheora scáileáin agus méarchláir freagraí na crosfhocal a chlóscríobh go díreach sna réimsí téacs thíos. TRASNA leideanna SÍOS leideanna

TRASNA

5 trasna: Monatóireacht ar ghníomhartha bogearraí atá ag rith le haghaidh patrúin oibríochta mailíseacha. (14 litir):

8 trasna: Sraith bogearraí a scanann agus a chosnaíonn críochphointí ó bhrattaí leochaileachta. (11 litir):

SÍOS

1 síos: Rabhadh slándála a aicmíonn bogearraí sábháilte go mícheart mar bhogearraí mailíseacha. (14 litir):

2 síos: Íoslódálacha rialta sainmhínithe a chothaíonn bunachar sonraí na mbagairtí. (13 litir):

3 síos: Timpeallacht fhíorúil thástála shlán ina ritear cód nach bhfuil iontaofa go sábháilte. (12 litir):

4 síos: Lorg uathúil chripteagrafach bunachair a úsáidtear chun bagairtí aitheanta a aithint. (12 litir):

6 síos: Comhaid amhrasacha a theorannú chun nochtadh an chórais áitiúil a sheachaint. (9 litir):

7 síos: Anailís rialachbhunaithe a chuireann comhaid le leaganacha amhrasacha cóid in iúl. (10 litir):

Seicphointe 6: Cuardach focal i bhfolach

Aimsigh na 8 dtéarma eochair-fhoclóra atá i bhfolach san eangach thíos. Is féidir focail a bheith cothrománach, ingearach, nó trasnánach.

B R E A G D H E A R F A C H Y

E S I S I A H U I N I S O Y W

S H T X H E O R A S T A I C A

P U N N Z O I Q T I P V U O U

U K A E P M K A N V G G P Q X

Y J K V J Y W Y P J I Z I J N

A E I A S A J F W E K Z K E K

Q N J S A E R I V H T I R F A

F O K N D N C D H I B A P R L

H M I N I A G A C S O B P W T

I S C A N A D H I O M P A I R

Y F Y C U A R A N T I N S G X

W H N U A S H O N R U I T H E

F R T N U K R D T S L P L M S

H K P H Y P L W U N Y Q Q B A

LIOSTA FOCAL FOCLÓIRE

SINIUHAISISE HEORASTAIC BOSCAGAINIMH SCANADHIOMPAIR NUASHONRUITHE BREAGDHEARFACH CUARANTIN FRITHVIREAS

Seicphointe 6, rogha eile: Meaitseáil foclóra inrochtana

Meaitseáil gach ceann de na 8 dtéarma foclóra ón Cuardach Focal lena sainmhíniú ceart trí scríobh na litreach (A-H) sa spás folamh.

TÉARMAÍ FOCLÓIRE

A. SINIUHAISISE

B. HEORASTAIC

C. BOSCAGAINIMH

D. SCANADHIOMPAIR

E. NUASHONRUITHE

F. BREAGDHEARFACH

G. CUARANTIN

H. FRITHVIREAS

SAINMHÍNITHE AGUS GLEANNTA MEAITSEÁLA

1. Monatóireacht ar ghníomhartha bogearraí atá ag rith le haghaidh patrúin oibríochta mailíseacha.

2. Sraith bogearraí a scanann agus a chosnaíonn críochphointí ó bhrattaí leochaileachta.

3. Íoslódálacha rialta sainmhínithe a chothaíonn bunachar sonraí na mbagairtí.

4. Anailís rialachbhunaithe a chuireann comhaid le leaganacha amhrasacha cóid in iúl.

5. Comhaid amhrasacha a theorannú chun nochtadh an chórais áitiúil a sheachaint.

6. Lorg uathúil chripteagrafach bunachair a úsáidtear chun bagairtí aitheanta a aithint.

7. Timpeallacht fhíorúil thástála shlán ina ritear cód nach bhfuil iontaofa go sábháilte.

8. Rabhadh slándála a aicmíonn bogearraí sábháilte go mícheart mar bhogearraí mailíseacha.

Seicphointe 7: Dúshlán focal measctha

Dí-mheascaigh na litreacha thíos chun príomhchoincheapa agus téarmaí cibearshlándála a nochtadh. Scríobh do chuid freagraí sna boscaí ionchuir a sholáthraítear.

1. SHIUIAISSNEI
2. HOAGBIMSINAC
3. UNRIUHEANHOTS
4. ANIRTNCUA
5. ASCERTAHIO
6. DHPAAAIIMSCORN
7. FCRBAREHDAEAHG
8. EISVIFHRART

Gníomhaíocht bhreise: Smaoinigh go tapa

3 FHREAGRA DO GACH CATAGÓIR. BUAILEANN AN CHÉAD DUINE A LÍONANN AN LIOSTA.

1	Cúiseanna le bogearraí a nuashonrú			
2	Daoine ar féidir leat cabhair TF a iarraidh orthu			
3	Rudaí le déanamh nuair a aimsíonn an frithvíreas rud éigin			
4	Comharthaí víris ríomhaire			
5	Rudaí a chuirtear i gcarntha			
6	Áiteanna ina bhfolaíonn víris			
7	Faisnéis nár cheart duit a roinnt choíche			
8	Cineálacha bogearraí mailíseacha			
9	Uirlisí slándála a bhfuil aithne agat orthu			
10	Rudaí a scanann frithvíreas			
11	Rudaí a dhéanann tú cúltaca díobh			
12	Feistí ar féidir hacáil a dhéanamh orthu			
13	Cláir fhrithvíorais a bhfuil aithne agat orthu			
14	Cúiseanna le rabhaidh bhréagacha			
15	Nósanna sábháilte is féidir leat a thosú inniu			

Seicphointe 8: Cás-staidéir ar chibearshlándáil

Cuir na coincheapa a d'fhoghlaim tú i bhfeidhm chun na cásanna fíorshaoil thíos a réiteach.

CÁS-STAIDÉAR 1: SCANADH SÍNITHE VS. SCANADH HEURISTIGH



Cás: Íoslódálann fostaí fóntais saincheaptha a thóg foireann eile go hinmheánach. Éiríonn leis an scanóir sínithe é a rith, ach cuireann an scanóir heorastúil bratach air mar rud amhrasach.

Ceist phlé: Mínigh cén fáth ar tharla sé seo, agus conas a fhíorú an bhfuil an comhad sábháilte.

CÁS-STAIDÉAR 2: TORTHAÍ BRÉAGA DEARFACHA A LÁIMHSEÁIL



Cás: Tiomsaíonn forbróir bogearraí a iarratas. Cuireann an frithvíreas córais bratach ar an gcomhad inrite nua mar bhogearraí mailíseacha agus cuireann sé i gcarntha é.

Ceist phlé: Déan achoimre ar na rioscaí a bhaineann le liostú bán, agus déan cur síos ar an gcosán ceart réitigh.

Seicphointe 9: Díchódaigh an cód

Cosnaíonn gairmí cibearshlándála sócmhainní líonra ó aisteoirí bagartha ar líne. Úsáid an eochair Litir-go-Uimhir thíos chun an teachtaireacht a dhíchódú trí na litreacha comhfhreagracha a scríobh sna spásanna folmha.

EOCHAIR CHRIPTITHE LITIR-GO-UIMHIR

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

1	9	18	9	7	8		2	15	7	5	1	18	18	1	9

13	1	9	12	9	19	5	1	3	8	1		14	21	1		12	5

8	5	15	18	1	19	20	1	9	3

Teachtaireacht díchódaithe:

COMHAIRLE: FREAGRAÍONN GACH UIMHIR DO SHUÍOMH NA LITRE SIN SAN AIBÍTIR (M.SH. 1 = A, 2 = B, 26 = Z).

Seicphointe 10: Ceisteanna coitianta faoi chibearshlándáil – bunleibhéal (Cuid A)

Athbhreithnigh ceisteanna agus freagraí coitianta maidir le laghdú bagairtí ar líne.

Q1: Conas a aithníonn bogearraí frithvíorais bogearraí mailíseacha?

Aithníonn sé bogearraí mailíseacha trí mheaitseáil sínithe bunachair sonraí, anailís ar leagan amach cóid eurasach, agus monatóireacht iompair fíor-ama.

Q2: Cad is brath bunaithe ar shínithe ann?

Is modh scanta é a mheaitseálann haisis chomhaid chripteagrafacha le liostaí bunachair sonraí de bhagairtí aitheanta bogearraí mailíseacha.

Q3: Cad é scanóir heoragnóiseach?

Déanann eurasachtaí struchtúr comhaid agus treoracha cóid a anailísiú, ag marcáil patrúin amhrasacha atá coitianta i leaganacha bogearraí mailíseacha.

Q4: Cad is brí leis nuair a chuirtear comhad i gcuarantín?

Bogann an frithvíreas an comhad go fillteán slán scoite, ag blocáil forghníomhaithe chun an córas oibriúcháin a chosaint.

Q5: Cad é bréagdheimhneach frithvíorais?

Is earráid é ina ndéantar bogearraí dlisteanacha sábháilte a mharcáil go mícheart mar bhogearraí mailíseacha ag algartaim scanta.

Seicphointe 10: Ceisteanna coitianta faoi chibearshlándáil – bunleibhéal (Cuid B)

Athbhreithnigh ceisteanna agus freagraí coitianta maidir le laghdú bagairtí ar líne.

Q6: Conas a chosnaíonn monatóireacht iompair córais?

Déanann sé monatóireacht fíor-ama ar bhogearraí atá ag rith, ag blocáil próiseas a dhéanann iarracht athruithe amhrasacha cosúil le cód a insteallú.

Q7: Cén fáth a bhfuil tástáil bosca gainimh tábhachtach?

Rithtear comhaid neamhiontaofa i meaisín fíorúil scoite le bosca gainimh, ag breathnú ar ghníomhartha go sábháilte gan nochtadh don chóras.

Q8: Cé chomh minic is ba cheart sainmhínithe frithvíorais a nuashonrú?

Ba cheart do scanóirí sainmhínithe a nuashonrú gach lá nó gach uair an chloig chun saghasanna nua-aimsithe bogearraí mailíseacha a aithint.

Q9: Cad é an difríocht idir frithvíreas agus EDR?

Díríonn frithvíreas ar scanadh comhad, agus soláthraíonn Endpoint Detection and Response (EDR) rianú agus coinneáil bagairtí ar fud an líonra.

Q10: An féidir liom dhá chlár fhrithvíreas a rith le chéile?

Ní hea. Cruthaíonn dhá scanóir ghníomhacha coinbhleachtaí córais, moillíonn siad feidhmíocht, agus féadann siad oibríochtaí a chéile a bhlocáil.

Seicphointe 10: Ceisteanna coitianta faoi shlándáil – ardleibhéal (Cuid C)

Déan iniúchadh ar ghnéithe teicniúla ardleibhéil de chreataí slándála, anailís bogearraí mailíseacha, agus comhlíonadh sonraí.

Q1: Conas a íoslaghdaíonn rialacha heoracha seachaint bagairtí?

Déanann eurasachtaí patrúin ghinearálta bagartha a anailísiú seachas sínithe ar leith, ag breith ar leaganacha athraithe de theaghlaigh aitheanta bogearraí mailíseacha.

Q2: Cad is víreas polaimorfach ann?

Is bogearraí mailíseacha iad a athraíonn a leagan amach comhaid agus a ghnáthamh díchriptithe le gach rith, rud a fhágann go bhfuil scanadh sínithe neamhéifeachtach.

Q3: Conas a bhraitheann bosca gainimh seachaint VM?

Insamhlaíonn boscaí gainimh nua-aimseartha cliceanna luiche agus am oibre an chórais, ag cur dallamullóg ar bhogearraí mailíseacha atá deartha chun folaigh nuair a ritheann siad i meaisíní fíorúla.

Q4: Cad iad formáidí íoslódála nuashonruithe sínithe?

Is comhaid dhifríochta dhénártha incriminteacha éadroma a bhíonn i nuashonruithe de ghnáth, rud a íoslaghdaíonn ídiú bandaleithid líonra cliant.

Q5: Conas a bhainistíonn gníomhairí críochphointe scanadh áitiúil?

Déanann gníomhairí seiceálacha éadroma cúlra, ag aistriú cuardaigh hash cripteagrafacha dhomhain chuig bunachair sonraí bagartha scamall.

Seicphointe 10: Ceisteanna coitianta faoi shlándáil – ardleibhéal (Cuid D)

Déan iniúchadh ar ghnéithe teicniúla ardleibhéil de chreataí slándála, anailís bogearraí mailíseacha, agus comhlíonadh sonraí.

Q6: Cad é scanadh braite rootkit?

Scanann sé táblaí cuimhne ar leibhéal na heithne, ag seachaint APInna an chórais oibriúcháin a ghabhann rootkits chun a snáitheanna gníomhacha a cheilt.

Q7: Conas a bhlocálann scanadh iompair bogearraí fuascailte?

Braitheann sé lúba uathoibrithe criptithe mais comhad, ag foirceannadh próiseas an óstaigh sula nglasáiltear bunachair sonraí an chórais.

Q8: Cad é fíorú deimhnithe sínithe cód?

Seiceálann scanóirí sínithe digiteacha cóid i gcoinne údarás deimhniúcháin fréimhe iontaofa, ag bailíochtú féiniúlacht fhorbróir na mbogearraí.

Q9: Conas a théann pacálaithe i bhfeidhm ar innill scanta?

Comhbhrúnn nó criptíonn pacálaithe ábhar mailíseach bogearraí mailíseacha. Caithfidh scanóirí an comhad a dhíphacáil sa chuimhne sular rithfear meaitseálacha sínithe.

Q10: Conas a uathoibríonn uirlisí EDR leithlisiú?

Cuireann gníomhairí EDR críochphointí ceilte i gcuarantín ar leibhéal an líonra, ag blocáil gluaiseachta cliathánaí agus ag ligean rochtain d'anailísithe.

Cuid 11: 10 bhFíric agus Léargas Cibearshlándála ón Domhan Fíor

Athbhreithnigh fíricí fíordhomhanda maidir le sáruithe slándála, sásraí cosanta, agus caighdeáin chomhlíonta.

1. EOLAS SLÁNDÁLA

Stórálann bunachair sonraí sínithe hais de bhogearraí mailíseacha aitheanta, mar sin ní bhraitear comhaid nua nó athraithe go dtí go nuashonraítear sainmhínithe.

2. EOLAS SLÁNDÁLA

Is féidir le hinnill eurasacha roinnt leaganacha nua bogearraí mailíseacha a mharcáil sula mbíonn sínithe ann, ar chostas níos mó dearfacha bréagacha.

3. EOLAS SLÁNDÁLA

Cuireann rabhaidh dhearfacha bhréige costas ar fhoirne TF: am a chaitear ag fíorú agus ag athchóiriú comhad a cuireadh i gcuarantín go mícheart.

4. EOLAS SLÁNDÁLA

Athraíonn bogearraí mailíseacha polaimorfacha a gcód le gach cóip, mar sin cuireann cosantóirí sínithe i bhfeidhm in éineacht le seiceálacha heoracha agus iompair.

6. EOLAS SLÁNDÁLA

Scríobhann údair bogearraí mailíseacha cóid shaincheaptha atá deartha chun timpeallachtaí bosca gainimh a sheiceáil, ag moill a chur ar fhorghníomhú chun amadóirí a sheachaint.

5. EOLAS SLÁNDÁLA

Seiceálann innill antaivíreas scamall-bhunaithe hashanna comhad amhrasta i gcoinne bunachar sonraí mór bagairtí ar líne beagnach i bhfíor-am.

7. EOLAS SLÁNDÁLA

Brúnn díoltóirí nuashonruithe sainmhínithe chuig críochphointí go rialta ionas gur féidir le scanóirí bagairtí nua-dhearbhaithe a aithint.

8. EOLAS SLÁNDÁLA

Díríonn monatóirí iompair bogearraí fuascailte ar ghlaonna API Win32 ar leith a bhaineann le criptiú comhad agus scriosadh cóipeanna scáileacha.

9. EOLAS SLÁNDÁLA

Is féidir le sínithe bailí cód baol bréag-dheimhneach a laghdú, ach scanáiltear comhaid shínithe fós, toisc gur féidir bogearraí mailíseacha a shíniú freisin.

10. EOLAS SLÁNDÁLA

Mionathraíonn rootkits struchtúir eithne an chórais, rud a éilíonn scanóirí speisialaithe ag am tosaithe chun iad a bhrath agus a ghlanadh.

Tagairtí teicniúla agus foinsí

Tá an treoirleabhar staidéir agus na mearaithe idirghníomhacha curtha le chéile ó chaighdeáin dhomhanda NIST, OWASP agus chomhlíonta príobháideachta sonraí. TAGAIRTÍ ACADÚLA AGUS TIONSCAIL

TAGAIRTÍ ACADÚLA AGUS TIONSCAIL

[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

Freagraí: Seicphointe 1 – Ilrogha

1 **Ceist 1** SÍNITHE **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Braitheann scanadh sínithe ar hashanna eolacha bunachair sonraí, agus teipeann air bogearraí mailíseacha anaithnide nó athraithe a bhrath. Luaigh: OWASP Secure Configuration.

2 **Ceist 2** EURASACHA **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Déanann heuristics anailís ar leagan amach cóid agus orduithe chun gnéithe amhrasacha de leaganacha nua bagartha a aithint. Luaigh: Center for Internet Security (CIS).

3 **Ceist 3** BOSCA GAINIMH A ÚSÁID **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Rithtear comhaid amhrasacha i mbosca gainimh i meaisín fíorúil iargúlta chun iompar forghníomhaithe a bhreathnú go sábháilte. Luaigh: NIST Digital Identity.

4 **Ceist 4** IOMPRAÍOCHTA **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Monatóiríonn scanadh iompair cláir atá ag rith i bhfíor-am chun athruithe córais neamhúdaraithe a bhlocáil. Luaigh: Center for Internet Security (CIS).

5 **Ceist 5** NUASHONRUITHE **Freagra ceart: A**

NÓTA DON MHÚINTEOIR

Íoslódálann scanóirí nuashonruithe sainmhínithe incriminteacha laethúla chun a bheith sioncronaithe le tírdhreach na mbagairtí. Luaigh: OWASP Secure Configuration.

Freagraí: Seicphointe 2 – Fíor nó Bréagach

6 **Ceist 6** SÍNITHE **Freagra ceart: Fíor**

NÓTA DON MHÚINTEOIR

Ríomhann uirlisí sínithe hashanna cripteagrafacha agus meaitseálann siad iad i gcoinne bunachair sonraí hashanna bagartha eolacha. Luaigh: OWASP Secure Configuration.

7 **Ceist 7** EURASACHA **Freagra ceart: Fíor**

NÓTA DON MHÚINTEOIR

Ritheann innill heuristic leaganacha amach atá bunaithe ar rialacha a fhéadann comhaid dhlisteanacha shábháilte a mharcáil mar chomhaid amhrasacha. Luaigh: Center for Internet Security (CIS).

8 **Ceist 8** BOSCA GAINIMH A ÚSÁID **Freagra ceart: Bréagach**

NÓTA DON MHÚINTEOIR

Ritheann bosca gainimh cód i gcoimeádán fíorúil, ag blocáil rochtain ar chomhroinnt líonra go docht. Luaigh: NIST Digital Identity.

9 **Ceist 9** IOMPRAÍOCHTA **Freagra ceart: Fíor**

NÓTA DON MHÚINTEOIR

Marcálann monatóireacht i bhfíor-am próisis atá ag rith a dhéanann iarracht scríobh neamhdhleathach nó glasáil comhaid. Luaigh: Center for Internet Security (CIS).

10 **Ceist 10** **Freagra ceart: Bréagach**

NÓTA DON MHÚINTEOIR

Ní stopann aon fhrithvíreas gach ionsaí zero-day; is féidir le bagairtí anaithnide sínithe agus heorastúlacht a sheachaint.

Eochracha foclóra agus rúibric mharcála

Rúbraic ghrádaithe don mhúinteoir: Bronn 1 phointe do gach meaitseáil cheart (8 pointe san iomlán) agus téarma comhthéacs (6 pointe san iomlán).

SEICPHOINTE 4: FREAGRAÍ – MEAITSEÁIL COINCHEAPA

D 1. Síniú haise	G 2. Heoiristící cóid	E 3. Bosca gainimh comhaid	C 4. Scanadh iompair
F 5. Nuashonruithe laethúla	H 6. Dearfach bréagach	A 7. Leithlisiú bagairtí	B 8. Uirlis frithvíreas

SEICPHOINTE 3: FREAGRAÍ – PRÍOMHTHÉARMAÍ

1 SÍNIÚ HAISISE	2 HEORASTAIC	3 BOSCA GAINIMH	4 IOMPAR
5 NUASHONRUITHE	6 BRÉAGDHEARFACH		

SEICPHOINTE 6, ROGHA EILE: FREAGRAÍ – MEAITSEÁIL FOCAL

1 D – SCANADHIOMPAIR	2 H – FRITHVIREAS	3 E – NUASHONRUITHE	4 B – HEORASTAIC
5 G – CUARANTIN	6 A – SINIUHAISISE	7 C – BOSCAGAINIMH	8 F – BREAGDHEARFACH

NÓTAÍ PLÉ DO MHÚINTEOIRÍ

Príomhthéarmaí:
Seiceáil an féidir leis na daltaí Síniú haise, Heoiristící cóid agus Bosca gainimh comhaid a mhíniú ina bhfocail féin agus sampla a thabhairt de gach ceann.

Cás-staidéir:
Iarr ar na daltaí a moltaí a bhunú ar fhíricí ón mbileog oibre, ní ar thuairimí.

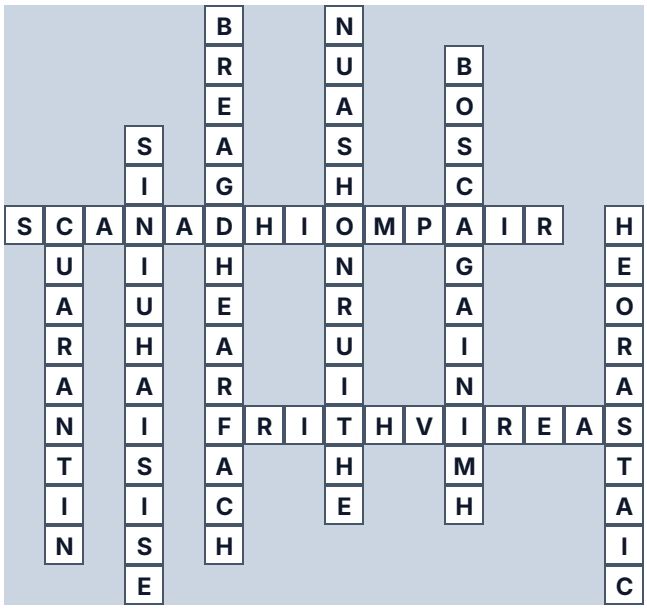
Measúnú foinsí:
Iarr ar na daltaí ráiteas amháin ar a laghad a fhíorú i bhfoinsí na bileoige agus pléigí cén fáth a bhféadfadh figiúirí, praghsanna agus rialacha athrú le himeacht ama.

Eochracha Puzal agus Nótaí don Mhúinteoir

CUR CHUN CINN FOCLÓIR CUARDAIGH

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

TUAIRISC CROSSWORD



TRASNA

5 trasna: SCANADHIOMPAIR Monatóireacht ar ghníomhartha bogearraí atá ag rith le haghaidh patrúin oibríochta mailíseacha. (14 litir)

8 trasna: FRITHVIREAS Sraith bogearraí a scanann agus a chosnaíonn críochphointí ó bhrattaí leochaileachta. (11 litir)

SÍOS

1 síos: BREAGDHEARFACH Rabhadh slándála a aicmíonn bogearraí sábháilte go mícheart mar bhogearraí mailíseacha. (14 litir)

2 síos: NUASHONRUITHE Íoslódálacha rialta sainmhínithe a chothaíonn bunachar sonraí na mbagairtí. (13 litir)

3 síos: BOSCAGAINIMH Timpeallacht fhíorúil thástála shlán ina ritear cód nach bhfuil iontaofa go sábháilte. (12 litir)

4 síos: SINIUHAISISE Lorg uathúil chripteagrafach bunachair a úsáidtear chun bagairtí aitheanta a aithint. (12 litir)

6 síos: CUARANTIN Comhaid amhrasacha a theorannú chun nochtadh an chórais áitiúil a sheachaint. (9 litir)

7 síos: HEORASTAIC Anailís rialachbhunaithe a chuireann comhaid le leaganacha amhrasacha cóid in iúl. (10 litir)

Eochair na bhfocal measctha agus réiteach an chóid

Eochair ghrádaithe don ghníomhaíocht dhíchuachta foclóra agus don Dúshlán Cód Rúnda.

EOCHAIR NA bhFOCAL DÍSCRAMBLAITHE

1. SHIUIAISSNEI — SINIUHAISISE
2. HOAGBIMSINAC — BOSCAGAINIMH
3. UNRIUHEANHOTS — NUASHONRUITHE
4. ANIRTNCUA — CUARANTIN
5. ASCERTAHIO — HEORASTAIC
6. DHPAAAIIMSCORN — SCANADHIOMPAIR
7. FCRBAREHDAEAHG — BREAGDHEARFACH
8. EISVIFHRART — FRITHVIREAS

EOCHAIR DHÚSHLÁN AN CHÓID RÚNDA

"AIRIGH BOGEARRAI MAILISEACHA NUA LE HEORASTAIC"

Freagraí na gcás-staidéar

A Cás-staidéar 1: Scanadh sínithe vs. scanadh heuristigh

Réiteach don mhúinteoir

TREOIRLÍNE GRÁDÚ

Ba cheart do fhreagraí na mac léinn na pointí seo a leanas a chlúdach:

- Anailís cháis: Íoslódálann fostaí áirge saincheaptha a thóg foireann eile go hinmheánach. Ritheann an scanóir sínithe é, ach marcálann an scanóir heorastúil é mar rud amhrasach.
- Straitéis agus réiteach molta: Cén fáth ar tharla sé: Seiceálann scanadh sínithe haiseanna comhaid; ós rud é go bhfuil sé saincheaptha, níl sé i mbunachar sonraí na mbagairtí. Déanann heorastaicí anailís ar struchtúr agus mharcáil siad gníomhartha amhrasacha (m.sh. scríobh clárlainne). Fíorú: Rith an comhad i mbosca gainimh chun gníomhartha a bhreathnú, seiceáil sínithe digiteacha, agus cuir an haiseach faoi bhráid tairseacha faisnéise bagartha.

B Cás-staidéar 2: Torthaí bréaga dearfacha a láimhseáil

Réiteach don mhúinteoir

TREOIRLÍNE GRÁDÚ

Ba cheart do fhreagraí na mac léinn na pointí seo a leanas a chlúdach:

- Anailís cháis: Tiomsaíonn forbróir bogearraí a fheidhmchlár. Marcálann antaivíreas an chórais an comhad inrite nua mar bhogearraí mailíseacha agus cuireann sé i gcoraintín é.
- Straitéis agus réiteach molta: Rioscaí an liosta cheadaithe: Is féidir le scanóirí a sheachaint cód fíor ionfhabhtaithe a ligean le rith. Cosán réitigh: Cuir an comhad faoi bhráid an díoltóra antaivíris le haghaidh anailíse, sínigh an cód go digiteach trí údaráis dheimhniúcháin, agus cumraigh eisceachtaí fillteáin sonracha go sealadach seachas an t-antaivíreas a mhúchadh.