Enw: _____ Dyddiad: _____ Sgôr: _____

Y We Dywyll yn erbyn y We Ddofn: Diogelwch a Gwahaniaethau

Mynegeio peiriannau chwilio, cronfeydd data'r we ddofn, llwybro nionyn Tor, anhysbysrwydd rhwydwaith a risgiau

TROSOLWG DYSGU Y WE DYWYLL A'R WE DDOFN

WEDI'I DDIOGELU

AMGRYPTIO DATA

Safon AES 256-did

YN CYDYMFFURFIO

SAFONAU BYD-EANG

Fframweithiau GDPR a CCPA

DIM YMDDIRIEDAETH

POLISI MYNEDIAD

Dilysu Aml-ffactor

Croeso! Mae'r pecyn gweithgareddau hwn yn eich tywys drwy'r gwahaniaethau rhwng y We Ddofn a'r We Dywyll. Byddwch yn archwilio cronfeydd data heb eu mynegeio, Llwybro Onion yn y porwr Tor, parthau cryptograffig .onion a risgiau diogelwch anhysbysrwydd.

PWYNTIAU GWIRIO'R DAFLEN WAITH

- [ ] **Rhan 1-4: Meistroli seiberddiogelwch ac atal bygythiadau.**
- [ ] **Rhan 5-7: Datrys posau croesair a chwilair.**
- [ ] **Rhan 8-9: Datrys astudiaethau achos a her y seiffr.**
- [ ] **Rhan 10: Adolygu tudalennau Cwestiynau Cyffredin sylfaenol ac uwch.**
- [ ] **Rhan 11: Archwilio 10 ffaith ddiddorol o'r byd go iawn.**
- [ ] **Bonws: her Meddwl yn Gyflym.**

Agorwch Ganllaw Seiberddiogelwch VPN.com

URL: https://www.vpn.com/cy/diogelwch-seiber/we-tywyll-vs-we-dwfn/

Eich Map Llwybr Dysgu Strategaeth y We Ddofn a'r We Dywyll

- Cyferbynnwch y we ddofn (cronfeydd data heb eu mynegeio) â'r we dywyll (gwasanaethau onion).
- Deall sut mae Onion Routing yn amgryptio ac yn trosglwyddo traffig rhwydwaith.
- Gwerthuso risgiau diogelwch cyrchu safleoedd rhwydwaith Tor heb eu dilysu.
- Defnyddiwch bolisïau porth diogel a blwch tywod ar gyfer cropian cudd-wybodaeth bygythiadau.
- Dadansoddwch fformat cyfeiriadau cryptograffig parthau gwasanaethau onion.

CYFARWYDDIADAU CANLLAW Y WE DDOFN A'R WE DYWYLL

Atebwch y cwestiynau amlddewis a gwir/gau, cwblhewch y brawddegau llenwi bylchau gan ddefnyddio'r banc geiriau, parwch y diffiniadau, a datryswch y posau croesair a chwilair. Cymhwyswch eich gwybodaeth i breifatrwydd ar y we ddofn a'r we dywyll. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

CRONFEYDD DATA'R WE DDOFN YN ERBYN LLWYBRO ONION Y WE DYWYLL (CYFLWYNIAD)

Mae'r we ddofn yn cynnwys tudalennau heb eu mynegeio y tu ôl i gyfrineiriau a mewngofnodion, fel e-byst preifat neu byrth banc corfforaethol. Is-set o'r we ddofn yw'r we dywyll sydd wedi'i chuddio'n fwriadol, ac mae angen porwyr arbenigol (fel Tor) a rhwydweithiau onion i'w chyrchu'n ddienw.

DARLLENWCH BOB PWYNT GWIRIO YN OFALUS A DEWISWCH NEU YSGRIFENNWCH YR YMATEB CYWIR.

Pwynt Gwirio 1: Her Amlddewis

1. Beth sy'n gwahaniaethu'r we ddofn oddi wrth y we arwyneb?

- A. Nid yw tudalennau'r we ddofn wedi'u mynegeio gan beiriannau chwilio cyhoeddus
- B. Mae traffig y we ddofn yn anghyfreithlon ac yn cael ei fonitro gan orfodi'r gyfraith
- C. Mae angen porwyr arbenigol fel Tor i gyrchu gwefannau'r we ddofn
- D. Mae tudalennau'r we ddofn bob amser yn llwytho'n gyflymach na thudalennau'r we arwyneb

2. Sut mae cyrchu'r we dywyll?

- A. Drwy borwyr arbenigol sy'n defnyddio rhwydweithiau llwybro nionyn
- B. Drwy ffurfweddu gosodiadau DNS wedi'u teilwra ar lwybryddion safonol
- C. Drwy gonsolau chwilio preifat ar y we arwyneb sydd ar gael drwy wahoddiad yn unig
- D. Drwy osod estyniad porwr safonol i rwystro hysbysebion

3. Pa strwythur sy'n ffurfio'r gyfran fwyaf o'r we ddofn?

- A. Cronfeydd data defnyddwyr a ddiogelir gan gyfrinair a chyfrifon preifat
- B. Fforymau marchnad ddu anghyfreithlon sy'n masnachu nwyddau anghyfreithlon
- C. Protocolau rhannu ffeiliau cymar-i-gymar heb eu hamgryptio
- D. Cronfeydd data celc peiriannau chwilio cyhoeddus

4. Beth mae Onion Routing yn ei wneud i draffig rhwydwaith?

- A. Mae'n amgryptio pecynnau ac yn eu llwybro drwy sawl cyfnewidydd
- B. Mae'n cynyddu cyflymder lawrlwytho drwy osgoi nodau'r ISP
- C. Mae'n mapio rhifau cyfresol caledwedd dyfeisiau i gofnodion IP
- D. Mae'n dileu cwcis y porwr gwe ar ôl pob clic

5. Pa ôl-ddodiad parth a ddefnyddir ar rwydweithiau Tor yn unig?

- A. Yr estyniad lefel uchaf cryptograffig .onion
- B. Yr estyniad masnachol .com hirsefydlog safonol
- C. Estyniad blockchain datganoledig .eth Web3
- D. Yr estyniad technoleg cod gwlad .ai

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn Gwir/Gau 6

6. Mae'r we ddofn a'r we dywyll yn cyfeirio at yr un rhan o'r rhwydwaith.

- ( ) Gwir
- ( ) Gau

7 Cwestiwn Gwir/Gau 7

7. Mae pyrth mewnrwyd corfforaethol yn rhan o'r we ddofn.

- ( ) Gwir
- ( ) Gau

8 Cwestiwn Gwir/Gau 8

8. Mae llwybro onion yn dadgryptio pecynnau data'n llwyr ym mhob nod tramwy.

- ( ) Gwir
- ( ) Gau

9 Cwestiwn Gwir/Gau 9

9. Mae cyrchu'r we dywyll yn datgelu dyfeisiau i risgiau maleiswedd uchel.

- ( ) Gwir
- ( ) Gau

10 Cwestiwn Gwir/Gau 10

10. Mae peiriannau chwilio gwe safonol yn cropian ac yn mynegeio gwefannau nionyn.

- ( ) Gwir
- ( ) Gau

Pwynt Gwirio 3: Mewnosod Termau Allweddol

Darllenwch bob brawddeg isod a llenwch y bwlch gyda'r term cywir o'r Banc Geiriau.

1. Mae pyrth banc preifat i'w cael yn y rhan heb ei mynegeio, sef _____ .

2. Mae nodau Tor arbenigol yn lletya gwasanaethau cudd mewn rhan o'r rhyngrwyd o'r enw _____ .

3. Mae gwefannau Tor yn defnyddio'r estyniad lefel uchaf cryptograffig _____ .

4. Yr enw ar anfon traffig drwy lwybr amlhaenog wedi'i amgryptio yw _____ .

5. Mae peiriannau chwilio'r we arwyneb yn cropian tudalennau sydd wedi'u _____ yn gyhoeddus.

6. Mae rhwydweithiau onion yn amgryptio cyfeiriadau IP cleientiaid i gynnal _____ defnyddwyr.

BANC GEIRIAU GEIRFA

.ONION | ANHYSBYSRWYDD | CRONFA DDATA | GWE DYWYLL | GWE DDOFN | LLWYBRO ONION | MYNEGEIO | NOD MYNEDIAD

Ysgrifennwch eich atebion yma:

1.

2.

3.

4.

5.

6.

Pwynt Gwirio 4: Paru Cysyniadau Diogelwch

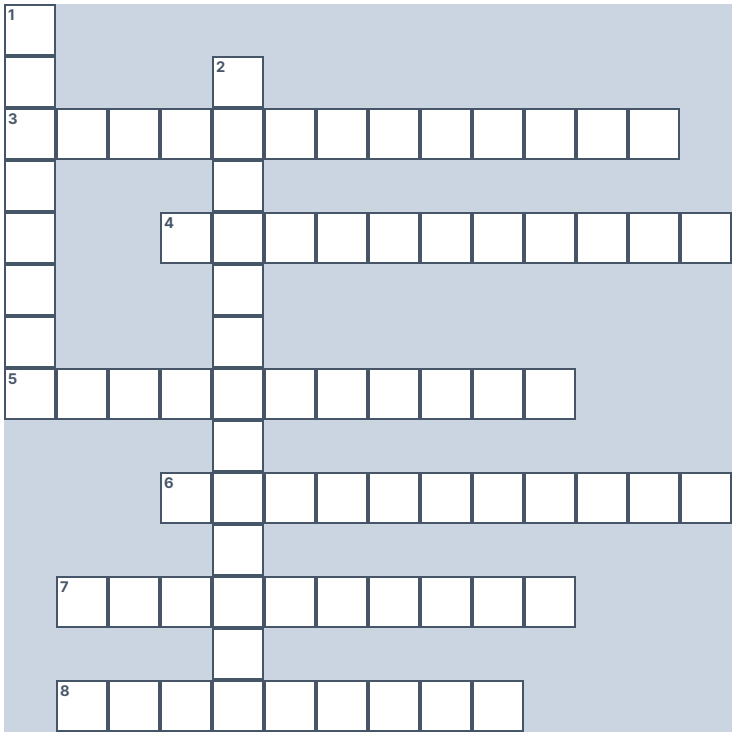
PARU DIFFINIADAU

Parwch bob term geirfa ar y chwith â'i ddiffiniad cywir ar y dde drwy ysgrifennu'r llythyren gyfatebol (A-H) yn y blwch mewnbwn y gellir ei lenwi.

☐	1. Rhan o'r We Ddofn	A	Rhan o'r rhwydwaith wedi'i hamgryptio sydd ar gael drwy borwyr arbennig yn unig.
☐	2. Porth y We Dywyll	B	Amgryptio data mewn haenau a'i drosglwyddo drwy dri nod.
☐	3. Estyniad Onion	C	Storfa gefn ddiogel sy'n cynnal cofnodion system heb eu mynegeio.
☐	4. Llwybro Tor	D	Ôl-ddodiad parth lefel uchaf cryptograffig a ddefnyddir ar rwydweithiau Tor.
☐	5. Tudalennau wedi'u Mynegeio	E	Y nod mynediad a ddefnyddir i gyrchu rhwydwaith Tor.
☐	6. Anhysbysrwydd Defnyddwyr	F	Cynnwys y we arwyneb wedi'i gasglu ac y gellir ei chwilio ar Google.
☐	7. Cronfa Ddata Breifat	G	Cadw cyfeiriadau IP cyhoeddus cleientiaid yn gudd rhag gweinyddion.
☐	8. Porth Mynediad	H	Cynnwys gwe heb ei fynegeio fel mewngofnodion preifat, e-byst a chofnodion cronfeydd data.

Pwynt Gwirio 5: Pos Croesair

Datryswch y croesair drwy deipio llythrennau yn y blychau gwyn gweithredol. Mae'r rhifau'n cyfateb i'r cliwiau isod.



CLIWIAU AR DRAWS

3. Ôl-ddodiad parth lefel uchaf cryptograffig a ddefnyddir ar rwydweithiau Tor (13)

4. Cynnwys y we arwyneb wedi'i gasglu ac yn chwiliadwy ar Google (11)

5. Y man cychwyn a ddefnyddir i ymuno â rhwydwaith Tor (11)

6. Storfa ôl-ben ddiogel sy'n lletya cofnodion system heb eu mynegeio (11)

7. Amgryptio data mewn haenau a'i drosglwyddo drwy dri nod (10)

8. Rhan o rwydwaith wedi'i hamgryptio y gellir ei chyrraedd drwy borwyr arbennig yn unig (9)

CLIWIAU I LAWR

1. Cynnwys gwe heb ei fynegeio fel mewngofnodi preifat, e-byst a chofnodion cronfeydd data (8)

2. Cadw cyfeiriadau IP cyhoeddus cleientiaid yn gudd rhag gweinyddion (13)

Pwynt Gwirio 5, dewis arall: Cliwiau Croesair Hygyrch

Gall defnyddwyr darllenwyr sgrin a bysellfwrdd deipio atebion y croesair yn uniongyrchol yn y meysydd testun isod.

CLIWIAU AR DRAWS

3 ar draws: Ôl-ddodiad parth lefel uchaf cryptograffig a ddefnyddir ar rwydweithiau Tor (13 llythyren):

4 ar draws: Cynnwys y we arwyneb wedi'i gasglu ac yn chwiliadwy ar Google (11 llythyren):

5 ar draws: Y man cychwyn a ddefnyddir i ymuno â rhwydwaith Tor (11 llythyren):

6 ar draws: Storfa ôl-ben ddiogel sy'n lletya cofnodion system heb eu mynegeio (11 llythyren):

7 ar draws: Amgryptio data mewn haenau a'i drosglwyddo drwy dri nod (10 llythyren):

8 ar draws: Rhan o rwydwaith wedi'i hamgryptio y gellir ei chyrraedd drwy borwyr arbennig yn unig (9 llythyren):

CLIWIAU I LAWR

1 i lawr: Cynnwys gwe heb ei fynegeio fel mewngofnodi preifat, e-byst a chofnodion cronfeydd data (8 llythyren):

2 i lawr: Cadw cyfeiriadau IP cyhoeddus cleientiaid yn gudd rhag gweinyddion (13 llythyren):

Pwynt Gwirio 6: Chwilair Geiriau Cudd

Dewch o hyd i'r 8 term geirfa allweddol sydd wedi'u cuddio yn y grid isod. Gall geiriau fod yn llorweddol, yn fertigol neu'n groeslinol.

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

RHESTR GEIRIAU GEIRFA

GWEDDOFN, GWEDYWYLL, ESTYNIADONION, LLWYBROTOR, MYNEGEIEDIG, ANHYSBYSRWYDD, CRONFADDATA, NODMYNEDIAD

Pwynt Gwirio 6, dewis arall: Paru Geirfa Hygyrch

Parwch bob un o'r 8 term geirfa o'r Chwilair â'i ddiffiniad cywir drwy ysgrifennu'r llythyren (A-H) yn y bwlch.

TERMAU GEIRFA

A. GWEDDOFN

B. GWEDYWYLL

C. ESTYNIADONION

D. LLWYBROTOR

E. MYNEGEIEDIG

F. ANHYSBYSRWYDD

G. CRONFADDATA

H. NODMYNEDIAD

DIFFINIADAU A MEYSYDD PARU

1. Cadw cyfeiriadau IP cyhoeddus cleientiaid yn gudd rhag gweinyddion.

2. Storfa ôl-ben ddiogel sy'n lletya cofnodion system heb eu mynegeio.

3. Amgryptio data mewn haenau a'i drosglwyddo drwy dri nod.

4. Cynnwys gwe heb ei fynegeio fel mewngofnodi preifat, e-byst a chofnodion cronfeydd data.

5. Rhan o rwydwaith wedi'i hamgryptio y gellir ei chyrraedd drwy borwyr arbennig yn unig.

6. Ôl-ddodiad parth lefel uchaf cryptograffig a ddefnyddir ar rwydweithiau Tor.

7. Y man cychwyn a ddefnyddir i ymuno â rhwydwaith Tor.

8. Cynnwys y we arwyneb wedi'i gasglu ac yn chwiliadwy ar Google.

Pwynt Gwirio 7: Her Geiriau Cymysg

Dad-sgramblwch y llythrennau isod i ddatgelu cysyniadau a thermau allweddol seiberddiogelwch. Ysgrifennwch eich atebion yn y blychau mewnbwn a ddarperir.

1. FDDGOWNE
2. ONSITEIANONDY
3. MIEENYIGGDE
4. DTAAOFADCRN
5. YYWLWDGLE
6. OBYOTLLRRW
7. WYSBANRSDDHYY
8. IEDNDNYOADM

Gweithgaredd Bonws: Meddwl yn Gyflym

3 ATEB YM MHOB CATEGORI. Y PERSON CYNTAF I GWBLHAU'R RHESTR SY'N ENNILL.

1	Rhesymau dros gadw draw o'r we dywyll			
2	Pethau na all peiriant chwilio ddod o hyd iddynt			
3	Dyfeisiau y gellir eu hacio			
4	Rhesymau cyfreithlon dros ddefnyddio Tor			
5	Rhesymau dros ddiweddaru meddalwedd			
6	Arwyddion rhybudd mewn e-bost			
7	Pethau a werthir yn anghyfreithlon ar y we dywyll			
8	Pobl y gallwch ofyn iddynt am help TG			
9	Arferion diogel y gallwch eu dechrau heddiw			
10	Pethau i'w gwneud ar ôl gollyngiad data			
11	Pethau sy'n perthyn i'r we ddofn			
12	Gwefannau rydych chi'n eu defnyddio gyda mewngofnodi			
13	Geiriau sy'n ymwneud ag anhysbysrwydd			
14	Gwybodaeth na ddylech byth ei rhannu			
15	Pethau sy'n gorwedd 'o dan yr wyneb'			

Pwynt Gwirio 8: Astudiaethau Achos Seiberddiogelwch

Cymhwyswch y cysyniadau rydych wedi'u dysgu i ddatrys y senarios go iawn isod.

ASTUDIAETH ACHOS 1: NODI GOLLYNGIADAU DATA



Senario: Mae archwiliad diogelwch corfforaethol yn darganfod bod cofnodion sensitif o gronfa ddata cleientiaid yn cael eu masnachu ar farchnad onion. Nid yw'r data wedi'i fynegeio ar Google.

Cwestiwn Trafod: Esboniwch pa segmentau o'r we sydd dan sylw a sut y digwyddodd y gollyngiad hwn.

ASTUDIAETH ACHOS 2: ANHYSBYSRWYDD O'I GYMHARU Â RISGIAU MALEISWEDD



Senario: Mae dadansoddwr am wirio ffrydiau cudd-wybodaeth am fygythiadau ar wefan Tor. Mae'n lawrlwytho porwr Tor ac yn cyrchu'r wefan.

Cwestiwn Trafod: Gwerthuswch fanteision anhysbysrwydd ac amlinellwch y camau i liniaru maleiswedd.

Pwynt Gwirio 9: Dadgryptio'r Seiffr

Mae gweithiwr proffesiynol seiberddiogelwch yn diogelu asedau rhwydwaith rhag actorion bygythiad ar-lein. Defnyddiwch yr allwedd Llythyren-i-Rif isod i ddadgryptio'r neges drwy ysgrifennu'r llythrennau cyfatebol yn y bylchau gwag.

ALLWEDD AMGRYPTIO LLYTHRENNAU-I-RIFAU

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

3	1	4	23	3	8		1	14	8	25	19	2	25	19	18	23	25	4	4
7	25	4	1		12	12	23	25	2	18	15		15	14	9	15	14		
						4	9	15	7	5	12								

Neges wedi'i datgodio:

AWGRYM: MAE POB RHIF YN CYNRYCHIOLI SAFLE'R LLYTHYREN HONNO YN YR WYDDOR (E.E. 1 = A, 2 = B, 26 = Z).

Pwynt Gwirio 10: Cwestiynau Cyffredin Sylfaenol am Seiberddiogelwch (Rhan A)

Adolygwch gwestiynau ac atebion cyffredin am liniaru bygythiadau ar-lein.

Q1: Beth yw'r we ddofn?

Mae'r we ddofn yn cynnwys pob tudalen we na all peiriannau chwilio ei mynegeio, gan gynnwys bancio ar-lein, cronfeydd data e-bost a chyfnodolion y tu ôl i wal dalu.

Q2: Beth yw'r we dywyll?

Is-set fach o'r we ddofn yw'r we dywyll, wedi'i chuddio'n fwriadol ac y gellir ei chyrchu dim ond drwy borwyr arbenigol sy'n defnyddio rhwydweithiau onion.

Q3: Sut mae peiriannau chwilio'n mynegeio tudalennau?

Mae peiriannau'n rhedeg rhaglenni awtomataidd (pryfed) i ddilyn dolenni cyhoeddus, gan fynegeio tudalennau nad ydynt yn rhwystro cropian drwy gyfarwyddebau robot.

Q4: Pam yr ystyrir bod bancio ar-lein yn rhan o'r we ddofn?

Mae pyrth bancio y tu ôl i waliau mewngofnodi a chyfrineiriau, sy'n rhwystro peiriannau cyhoeddus rhag mynegeio tudalennau datganiadau cyfrif.

Q5: Beth yw Llwybro Onion porwr Tor?

Mae llwybro onion yn ddull trosglwyddo sy'n amgryptio traffig mewn haenau ac yn ei basio drwy drosglwyddyddion lluosog i guddio cyfeiriadau IP defnyddwyr.

Pwynt Gwirio 10: Cwestiynau Cyffredin Sylfaenol am Seiberddiogelwch (Rhan B)

Adolygwch gwestiynau ac atebion cyffredin am liniaru bygythiadau ar-lein.

Q6: A yw cyrchu'r we dywyll yn anghyfreithlon?

Na. Mae cael mynediad i'r we dywyll yn gyfreithlon yn y rhan fwyaf o wledydd, er bod cymryd rhan mewn marchnadoedd anghyfreithlon neu weithgareddau seiber anghyfreithlon wedi'i wahardd.

Q7: Pam mae gwefannau'r we dywyll yn araf i'w llwytho?

Caiff traffig ei lwybro a'i ddadgryptio drwy o leiaf dri chyfnewidydd byd-eang (mynediad, canol, allanfa), sy'n cynyddu hwyrni trosglwyddo.

Q8: Beth yw ystyr yr ôl-ddodiad parth .onion?

Mae'n ôl-ddodiad parth lefel uchaf arbenigol a ddefnyddir ar rwydweithiau Tor, sy'n pwyntio at gyfeiriadau a gynhyrchir yn gryptograffig yn hytrach na gweinyddion DNS safonol.

Q9: Pa risgiau sy'n gysylltiedig â dolenni'r we dywyll?

Nid oes gan wefannau unrhyw sgrinio diogelwch, gan amlygu defnyddwyr i gyfraddau uchel o heintio â maleiswedd, sgriptiau gwe-rwydo a sgamiau trafodion.

Q10: Pwy greodd brotocol llwybro rhwydwaith Tor?

Datblygwyd y dechnoleg yn wreiddiol gan U.S. Naval Research Laboratory yn y 1990au i ddiogelu cyfathrebiadau'r llywodraeth.

Pwynt Gwirio 10: Cwestiynau Cyffredin Uwch am Ddiogelwch (Rhan C)

Archwilio agweddau technegol uwch ar fframweithiau diogelwch, dadansoddi maleiswedd, a chydymffurfiaeth data.

Q1: Sut mae nodau canolraddol yn diogelu anhysbysrwydd Tor?

Mae pob nod yn dadgryptio un haen o ddata llwybro yn unig, gan ddysgu'r naid flaenorol a'r naid nesaf yn unig, byth y ffynhonnell a'r gyrchfan ill dwy.

Q2: Beth yw rôl y nod allanfa?

Mae'r nod allanfa yn dadgryptio haen olaf yr amgryptio, gan anfon y traffig allan i'r gweinydd cyrchfan cyhoeddus neu'r gweinydd onion.

Q3: Beth yw porth pontydd Tor?

Mae pontydd yn drosglwyddyddion mynediad Tor heb eu rhestru a ddefnyddir i osgoi rhwystrau ISP a sensoriaeth mewn rhanbarthau sy'n cyfyngu mynediad at borwr Tor.

Q4: Sut mae actorion y we dywyll yn camfanteisio ar arian cyfred digidol?

Mae actorion yn defnyddio arian cyfred digidol dienw i gyflawni masnachau ariannol ar farchnadoedd tywyll, gan osgoi gwiriadau trafodion bancio safonol.

Q5: Pam mae peiriannau chwilio safonol yn methu ag ymlusgo cronfeydd data dwfn?

Ni all ymlusgwyr fewnbynnu manylion mewngofnodi, datrys CAPTCHAs diogelwch, na rhedeg sgriptiau ymholiadau SQL ôl-ben sydd eu hangen i gyrchu cronfeydd data dwfn.

Pwynt Gwirio 10: Cwestiynau Cyffredin Uwch am Ddiogelwch (Rhan D)

Archwilio agweddau technegol uwch ar fframweithiau diogelwch, dadansoddi maleiswedd, a chydymffurfiaeth data.

Q6: Beth yw gweinydd cyfeiriadur mewn rhwydweithiau Tor?

Mae'n weinydd dibynadwy sy'n cynnal y rhestr o drosglwyddyddion mynediad, canol ac allanfa gweithredol a ddefnyddir gan gleientiaid i lunio llwybrau.

Q7: Sut mae actorion maleisus yn sniffian ar nodau ymadael?

Gall gweithredwyr nodau allanfa twyllodrus ryng-gipio traffig HTTP heb ei amgryptio wrth iddo adael rhwydwaith Tor, gan ddwyn enwau defnyddwyr a chwcis.

Q8: Beth yw'r gwahaniaeth rhwng Tor ac I2P?

Mae Tor yn defnyddio cyfeiriadur cyfnewidwyr canolog a nodau allanfa ar gyfer mynediad i'r we gyhoeddus, tra bo I2P yn defnyddio strwythur cymar-i-gymar datganoledig ar gyfer lletya mewnol.

Q9: Sut mae asiantaethau gorfodi'r gyfraith yn olrhain marchnadoedd y we dywyll?

Mae asiantaethau'n defnyddio dadansoddiad blockchain, yn lleoli gosodiadau lletya gweinyddion ffisegol, ac yn cynnal gweithrediadau abwyd i adnabod gweithredwyr.

Q10: Sut mae gollyngiadau DNS yn peryglu anhysbysrwydd y cleient?

Mae gollyngiadau DNS yn digwydd pan anfonir ymholiadau DNS y porwr yn uniongyrchol drwy'r ISP lleol yn hytrach na'u llwybro drwy rwydwaith Tor wedi'i amgryptio.

Rhan 11: 10 Ffaith a Mewnwelediad Seiberddiogelwch o'r Byd Go Iawn

Adolygwch ffeithiau o'r byd go iawn am dor-diogelwch, mecanweithiau amddiffyn, a safonau cydymffurfio.

1. CIPOLWG AR DDIOGELWCH

Mae'r we ddofn yn llawer mwy na'r we arwyneb y gellir chwilio ynddi, gan fod y rhan fwyaf o'r cynnwys y tu ôl i fewngofnodion a chronfeydd data.

2. CIPOLWG AR DDIOGELWCH

Rhan fach o'r we ddofn sydd wedi'i chuddio'n fwriadol yw'r we dywyll, a chyrhaeddir hi gydag offer fel Tor.

3. CIPOLWG AR DDIOGELWCH

Mae llwybro Tor yn amgryptio pecynnau data deirgwaith, gan blicio haenau amgryptio fel nionyn ym mhob nod cyfnewid.

4. CIPOLWG AR DDIOGELWCH

Tyfodd Tor o'r prosiect llwybro onion a gynhaliwyd gan U.S. Naval Research Lab, a rhyddhawyd ei god fel meddalwedd rydd. [1]

5. CIPOLWG AR DDIOGELWCH

Mae cyfeiriadau onion yn llinynnau alffaniwmerig 56 nod a gynhyrchir yn gryptograffig o barau allweddi cyhoeddus.

6. CIPOLWG AR DDIOGELWCH

Gall nodau allanfa ddarllen traffig testun clir, sy'n golygu bod TLS/HTTPS yn dal yn ofynnol ar Tor ar gyfer data sesiwn diogel.

7. MEWNWELEDIAD DIOGELWCH

Gwefannau mewnrwyd, gyriannau cwmwl a chronfeydd data preifat yw'r segmentau storio data mwyaf ar y we ddofn.

8. MEWNWELEDIAD DIOGELWCH

Mae peiriannau chwilio arbenigol fel DuckDuckGo yn rhedeg pyrth nionyn i ganiatáu chwiliadau dienw ar rwydweithiau Tor.

9. MEWNWELEDIAD DIOGELWCH

Mae dros 2 filiwn o ddefnyddwyr yn cysylltu â rhwydwaith Tor bob dydd i osgoi sensoriaeth a chynnal preifatrwydd cyfathrebu.

10. CIPOLWG AR DDIOGELWCH

Mae gweithrediadau gorfodi'r gyfraith byd-eang (fel Operation Bayonet) yn cau marchnadoedd tywyll mawr drwy atafaelu caledwedd lletya.

Cyfeiriadau a Ffynonellau Technegol

Mae'r canllaw astudio a'r posau rhyngweithiol wedi'u llunio o safonau byd-eang NIST, OWASP a chydymffurfio â phreifatrwydd data.

CYFEIRIADAU YSGOLHEIGAIDD A DIWYDIANT

[1] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

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

[5] 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

Allwedd Atebion: Pwynt Gwirio 1 – Amlddewis

1 **Mynegeio Chwilio** GWE DDOFN — Ateb Cywir: A

NODYN ADDYSGU

Mae tudalennau'r we ddofn y tu ôl i waliau mewngofnodi a chronfeydd data, gan atal pryfed chwilio rhag eu cropian. Ffynhonnell: IETF RFC 3986.

2 **Mynediad i Tor** GWE DYWYLL — Ateb Cywir: A

NODYN ADDYSGU

Mae'r we dywyll yn cynnwys gwasanaethau onion cudd y gellir eu cyrchu dim ond drwy borwyr fel Tor. Dyfyniad: IETF RFC 3986.

3 **Cronfeydd Data Dwfn** CRONFEYDD DATA — Ateb Cywir: A

NODYN ADDYSGU

Cyfrifon a ddiogelir gan gyfrinair a chofnodion corfforaethol yw'r rhan fwyaf o'r we ddofn. Ffynhonnell: NIST Digital Identity.

4 **Llwybro Onion** RHWYDWAITH TOR — Ateb Cywir: A

NODYN ADDYSGU

Mae llwybro onion yn amgryptio pecynnau data mewn haenau, gan eu trosglwyddo drwy nodau lluosog er mwyn anhysbysrwydd. Ffynhonnell: IETF RFC 3986.

5 **Parth Onion** ÔL-DDODIAD — Ateb Cywir: A

NODYN ADDYSGU

Mae ôl-ddodiad parth cryptograffig.onion yn llwybro traffig yn fewnol ar Tor heb DNS cyhoeddus. Dyfyniad: IETF RFC 3986.

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

6 **Segmentau Gwe** STRWYTHUR — **Ateb Cywir: Gau**

NODYN ADDYSGU

Mae'r we ddofn yn cwmpasu pob tudalen heb ei mynegeio, tra bo'r we dywyll yn is-ran onion fach, amgryptiedig. Dyfyniad: IETF RFC 3986.

7 **Mewnrwydi Corfforaethol** GWE DDOFN — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae gwefannau mewnrwyd y tu ôl i byrth cyfrinair ac nid ydynt wedi'u mynegeio, sy'n golygu eu bod yn perthyn i'r we ddofn. Ffynhonnell: NIST Digital Identity.

8 **Amgryptio Haenog** TROSGLWYDDYDDION — **Ateb Cywir: Gau**

NODYN ADDYSGU

Dim ond un haen llwybro y mae trosglwyddyddion onion yn ei dadgryptio i amddiffyn anhysbysrwydd y defnyddiwr, byth y pecyn cyfan. Ffynhonnell: IETF RFC 3986.

9 **Amlygiad i Faleiswedd** BYGYTHIADAU — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Nid oes gan farchnadoedd y we dywyll unrhyw hidlo diogelwch, ac maent yn cario risgiau eithafol o haint maleiswedd. Ffynhonnell: Center for Internet Security (CIS).

10 **Cwestiwn 10** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Nid yw ymlusgwyr peiriannau chwilio cyffredin yn defnyddio Tor, felly ni allant gyrraedd na mynegeio gwefannau .onion.

Allweddi Geirfa a Chyfarwyddyd Marcio

Cyfarwyddyd Marcio i Athrawon: Rhowch 1 pwynt am bob paru cywir (8 pwynt i gyd) a phob term cyd-destun (6 phwynt i gyd).

PWYNT GWIRIO 4: ALLWEDD PARU CYSYNIADAU

H 1. Rhan o'r We Ddofn	A 2. Porth y We Dywyll	D 3. Estyniad Onion	B 4. Llwybro Tor
F 5. Tudalennau wedi'u Mynegeio	G 6. Anhysbysrwydd Defnyddwyr	C 7. Cronfa Ddata Breifat	E 8. Porth Mynediad

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 GWE DDOFN	2 GWE DYWYLL	3 .ONION	4 LLWYBRO ONION
5 MYNEGEIO	6 ANHYSBYSRWYDD		

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 F – ANHYSBYSRWYDD	2 G – CRONFADDATA	3 D – LLWYBROTOR	4 A – GWEDDOFN
5 B – GWEDYWYLL	6 C – ESTYNIADONION	7 H – NODMYNEDIAD	8 E – MYNEGEIEDIG

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio Rhan o'r We Ddofn, Porth y We Dywyll a Estyniad Onion yn eu geiriau eu hunain a rhoi enghraifft o bob un.

Astudiaethau Achos:
Gofynnwch i fyfyrwyr gefnogi eu hargymhellion â ffeithiau o'r daflen waith yn hytrach na thybiaethau.

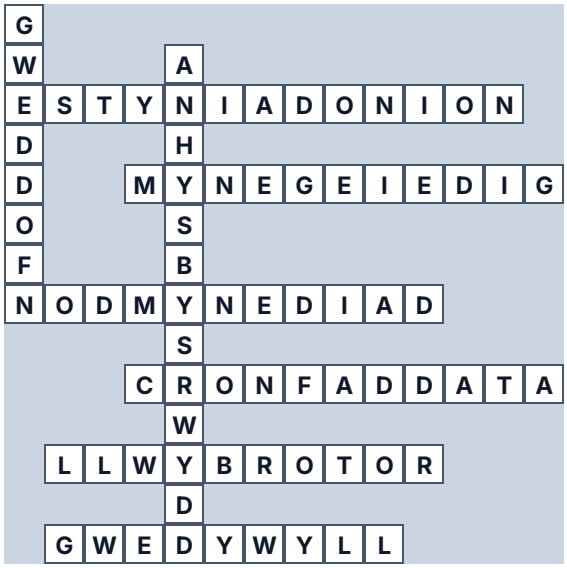
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

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

DATRYSIAD Y CROESAIR



CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

CLIWIAU AR DRAWS

3 ar draws: ESTYNIADONION Ôl-ddodiad parth lefel uchaf cryptograffig a ddefnyddir ar rwydweithiau Tor (13 llythyren)

4 ar draws: MYNEGEIEDIG Cynnwys y we arwyneb wedi'i gasglu ac yn chwiliadwy ar Google (11 llythyren)

5 ar draws: NODMYNEDIAD Y man cychwyn a ddefnyddir i ymuno â rhwydwaith Tor (11 llythyren)

6 ar draws: CRONFADDATA Storfa ôl-ben ddiogel sy'n lletya cofnodion system heb eu mynegeio (11 llythyren)

7 ar draws: LLWYBROTOR Amgryptio data mewn haenau a'i drosglwyddo drwy dri nod (10 llythyren)

8 ar draws: GWEDYWYLL Rhan o rwydwaith wedi'i hamgryptio y gellir ei chyrraedd drwy borwyr arbennig yn unig (9 llythyren)

CLIWIAU I LAWR

1 i lawr: GWEDDOFN Cynnwys gwe heb ei fynegeio fel mewngofnodi preifat, e-byst a chofnodion cronfeydd data (8 llythyren)

2 i lawr: ANHYSBYSRWYDD Cadw cyfeiriadau IP cyhoeddus cleientiaid yn gudd rhag gweinyddion (13 llythyren)

Allwedd Datrys Geiriau Cymysg a Seiffr

Allwedd marcio ar gyfer y gweithgaredd dad-sgramblo geirfa a'r Her Seiffr Gyfrinachol.

ALLWEDD DATRYS GEIRIAU CYMYSG

1. FDDGOWNE — GWEDDOFN
2. ONSITEIANONDY — ESTYNIADONION
3. MIEENYIGGDE — MYNEGEIEDIG
4. DTAAOFADCRN — CRONFADDATA
5. YYWLWDGLE — GWEDYWYLL
6. OBYOTLLRRW — LLWYBROTOR
7. WYSBANRSDDHYY — ANHYSBYSRWYDD
8. IEDNDNYOADM — NODMYNEDIAD

ALLWEDD HER Y SEIFFR CYFRINACHOL

"CADWCH ANHYSBYSRWYDD GYDA LLWYBRO ONION DIOGEL"

Allwedd Atebion yr Astudiaethau Achos

A Astudiaeth Achos 1: Nodi Gollyngiadau Data

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae archwiliad diogelwch corfforaethol yn darganfod bod cofnodion sensitif o gronfa ddata cleientiaid yn cael eu masnachu ar farchnad onion. Nid yw'r data wedi'i fynegeio ar Google.
- Strategaeth ac Ateb a Argymhellir: Segmentau Dan Sylw: Mae'r gronfa ddata breifat yn perthyn i'r we ddofn (heb ei mynegeio ond yn ddiogel). Mae'r farchnad sy'n masnachu'r data a ddygwyd ar y we dywyll (rhwydwaith onion). Sut y Digwyddodd: Aeth hacwyr heibio i amddiffynfeydd y gweinydd, dwyn y gronfa ddata o'r we ddofn, a'i rhestru'n ddienw ar y we dywyll i osgoi cael eu holrhain gan orfodi'r gyfraith.

B Astudiaeth Achos 2: Anhysbysrwydd o'i Gymharu â Risgiau Maleiswedd

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae dadansoddwr eisiau gwirio ffrydiau cudd-wybodaeth am fygythiadau ar wefan Tor. Mae'n lawrlwytho porwr Tor ac yn cael mynediad at y wefan.
- Strategaeth a Datrysiad a Argymhellir: Manteision: Mae Tor yn llwybro traffig drwy dri nod, gan guddio IP corfforaethol y dadansoddwr. Risgiau a Lliniaru: Nid oes sgrinio enw da ar ddolenni'r we dywyll. Rhaid i ddadansoddwyr redeg Tor y tu mewn i beiriannau rhithwir (VMs) ynysig, analluogi Javascript yng ngosodiadau Tor, ac osgoi llwytho unrhyw ffeiliau i lawr er mwyn diogelu'r rhwydwaith corfforaethol.