Enw: _____ Dyddiad: _____ Sgôr: _____

Dadansoddi Maleiswedd a Lliniaru Bygythiadau Canllaw

Ceffylau Troea, meddalwedd wystlo, ysbïwedd, rootkits, blychau tywod rhithwiroli, cyfyngu

TROSOLWG DYSGU DADANSODDI MALEISWEDD

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 ddadansoddi ac atal maleiswedd. Byddwch yn archwilio ysbïwedd, trojans, llwythi meddalwedd wystlo, offer peirianneg wrthdro, ymddygiad rootkits a strategaethau cyfyngu.

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/maleiswedd/

Eich Map Llwybr Dysgu Lliniaru Maleiswedd

- Gwahaniaethwch rhwng mathau o faleiswedd Trojan, mwydyn a rootkit.
- Rhowch weithredu rhithwiroli mewn blwch tywod ar waith ar gyfer dadansoddi cod.
- Lluniwch gynlluniau cyfyngu a glanweithio ar gyfer llwythi ransomware gweithredol.

CYFARWYDDIADAU'R CANLLAW DADANSODDI MALEISWEDD

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 liniaru maleiswedd. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

DADANSODDI MALEISWEDD A CHYFYNGU BYGYTHIADAU (CYFLWYNIAD)

Mae cod maleisus fel Trojans, mwydod a nwyddau pridwerth yn fygythiadau effaith uchel i bwyntiau terfyn a gweinyddion. Mae timau diogelwch yn dadansoddi maleiswedd mewn blychau tywod rhithwir ac yn gweithredu rheolaethau ynysu rhwydwaith cyflym i gyfyngu ar ledaeniad y llwyth.

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

Pwynt Gwirio 1: Her Amlddewis

1. **1. Beth yw nodwedd ddiffiniol ceffyl Troea?**
   - A. Mae'n ymddangos fel meddalwedd ddilys i dwyllo defnyddwyr i'w rhedeg
   - B. Mae'n atgynhyrchu'n awtomatig ar draws llinellau'r rhwydwaith lleol
   - C. Mae'n heintio ffeiliau mewn blychau tywod rhithwir ynysig
   - D. Mae'n rhyng-gipio traffig y darparwr gwasanaeth rhyngrwyd

2. **2. Pa fath o faleiswedd sy'n amgryptio ffeiliau ac yn mynnu taliad?**
   - A. Nwyddau pridwerth
   - B. Ysbïwedd
   - C. Rootkit
   - D. Hysbyswedd

3. **3. Beth sy'n cynrychioli ysbïwedd?**
   - A. Maleiswedd a gynlluniwyd i fonitro trawiadau bysell a gweithgareddau porwr defnyddwyr yn gyfrinachol
   - B. Cod rhaglen sy'n gweithredu y tu mewn i gynhwysydd rhithwir mewn blwch tywod
   - C. Diweddariadau gwrth-faleiswedd a lawrlwythwyd o gofrestrfeydd cronfeydd data
   - D. Addasu disgleirdeb y sgrin yn awtomatig

4. **4. Pam mae datblygwyr maleiswedd yn defnyddio rootkits?**
   - A. I guddio prosesau gweithredol a ffeiliau maleisus rhag y system weithredu
   - B. Cynyddu cyflymder prosesu'r CPU ar ddyfeisiau terfyn
   - C. Er mwyn gwneud copïau wrth gefn o ffeiliau cronfa ddata mewn cladgelloedd cwmwl diogel
   - D. Er mwyn gwella bywyd batri ar liniaduron

5. **5. Beth yw ystyr blwch tywod wrth ddadansoddi maleiswedd?**
   - A. Gweithredu ffeiliau amheus mewn cladgell rithwir ynysig i arsylwi ar eu hymddygiad yn ddiogel
   - B. Sganio hashes ffeiliau yn erbyn cronfeydd data bygythiadau hysbys
   - C. Adfer copïau wrth gefn o gronfeydd data ar ôl ymyrraeth
   - D. Datgysylltu llwybryddion y rhwydwaith lleol oddi wrth linellau cyhoeddus

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn 6

6. Mae angen rhyngweithio gan ddefnyddiwr dynol ar fwydod cyfrifiadurol i ymledu ar draws rhwydweithiau lleol.

○ Gwir ○ Gau

7 Cwestiwn 7

7. Mae meddalwedd hysbysebu bob amser yn ddiniwed ac nid yw'n olrhain ymddygiad defnyddwyr na hanes y porwr.

○ Gwir ○ Gau

8 Cwestiwn 8

8. Mae adfer copïau wrth gefn glân all-lein yn gadael i ddioddefwyr adfer ffeiliau wedi'u hamgryptio heb dalu'r pridwerth.

○ Gwir ○ Gau

9 Cwestiwn 9

9. Mae gwrthfeirws sy'n seiliedig ar lofnodion yn atal maleiswedd dim diwrnod yn ddibynadwy cyn bod unrhyw lofnod ar ei chyfer yn bodoli.

○ Gwir ○ Gau

10 Cwestiwn 10

10. Mae maleiswedd ddi-ffeil yn rhedeg sgriptiau maleisus yng nghof y system, gan osgoi ysgrifennu ffeiliau i'r ddisg.

○ 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. Enw maleiswedd wedi'i chuddio fel rhaglen ddiogel yw _____ .

2. Mae llwythi maleisus sy'n cloi systemau cronfa ddata er mwyn arian yn enghraifft o _____ .

3. Mae cofnodwyr bysellau sy'n cofnodi cyfrineiriau'n gyfrinachol yn fath o _____ .

4. Mae angen _____ i guddio'n ddwfn yng nghnewyllyn system weithredu.

5. Mae dadansoddi ffeiliau amheus mewn claddgell ynysig yn defnyddio _____ rhithwir.

6. Mae atal lledaeniad llwythi maleiswedd gweithredol yn golygu bod angen _____ y rhwydwaith ar unwaith.

BANC GEIRIAU GEIRFA

BLWCH TYWOD CEFFYL PREN CYFYNGU DIFFEIL MWYDYN RANSOMWEDD ROOTKIT YSBIWEDD

Ysgrifennwch eich atebion yma:

1. | **2.**

3. | **4.**

5. | **6.**

Pwynt Gwirio 4: Paru Cysyniadau Diogelwch

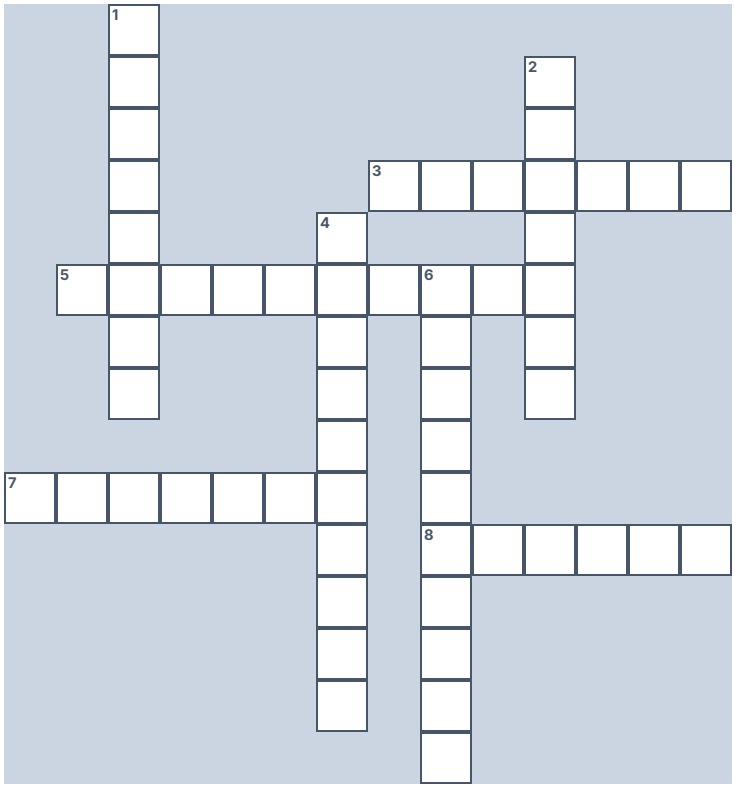
PARU DIFFINIADAU

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. CEFFYL PREN	A. Rhaglen sydd wedi'i chynllunio i fonitro a chofnodi gweithgarwch a mewnbynnau'r defnyddiwr yn gyfrinachol.
2. MEDDALWEDD WYSTLO	B. Maleiswedd sy'n gweithredu'n uniongyrchol yn y RAM i osgoi cael ei chanfod gan sganwyr disg.
3. YSBÏWEDD	C. Cyfyngu pwyntiau terfyn sydd wedi'u heintio i atal llwythi bygythiad rhag lledaenu.
4. ROOTKIT	D. Meddalwedd faleisus wedi'i chuddio fel rhaglen gyfleustodau ddiniwed neu ddefnyddiol.
5. BLWCH TYWOD	E. Maleiswedd hunanddyblygol sy'n lledaenu ar draws rhwydweithiau heb weithred ddynol.
6. CYFYNGU	F. Maleiswedd sy'n amgryptio storfa'r system ac yn mynnu taliad am ddarparu'r allwedd.
7. MWYDYN	G. Amgylchedd rhithwir ynysig a ddefnyddir i ddadansoddi ffeiliau maleisus yn ddiogel.
8. DI-FFEIL	H. Maleiswedd lechwraidd sy'n cuddio'n ddwfn yng nghnewyllyn y system i gadw rheolaeth weinyddol.

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. Maleiswedd sy'n rhedeg yn uniongyrchol yn y RAM i osgoi cael ei chanfod gan sganwyr disg. (7)

5. Meddalwedd faleisus wedi'i chuddio fel rhaglen ddiniwed neu ddefnyddiol. (10)

7. Maleiswedd lechwraidd sy'n cuddio'n ddwfn yng nghnewyllyn y system i gadw rheolaeth weinyddol. (7)

8. Maleiswedd sy'n ei dyblygu ei hun ac yn lledaenu ar draws rhwydweithiau heb weithred ddynol. (6)

CLIWIAU I LAWR

1. Rhaglen a gynlluniwyd i fonitro a chofnodi gweithgarwch a mewnbynnau defnyddwyr yn gyfrinachol. (8)

2. Ynysu dyfeisiau terfynol heintiedig i atal llwythi bygythiad rhag lledaenu. (7)

4. Amgylchedd rhithwir ynysig a ddefnyddir i ddadansoddi ffeiliau maleisus yn ddiogel. (10)

6. Maleiswedd sy'n amgryptio storfa'r system ac yn mynnu taliad am yr allwedd. (10)

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: Maleiswedd sy'n rhedeg yn uniongyrchol yn y RAM i osgoi cael ei chanfod gan sganwyr disg. (7 llythyren):

5 ar draws: Meddalwedd faleisus wedi'i chuddio fel rhaglen ddiniwed neu ddefnyddiol. (10 llythyren):

7 ar draws: Maleiswedd lechwraidd sy'n cuddio'n ddwfn yng nghnewyllyn y system i gadw rheolaeth weinyddol. (7 llythyren):

8 ar draws: Maleiswedd sy'n ei dyblygu ei hun ac yn lledaenu ar draws rhwydweithiau heb weithred ddynol. (6 llythyren):

CLIWIAU I LAWR

1 i lawr: Rhaglen a gynlluniwyd i fonitro a chofnodi gweithgarwch a mewnbynnau defnyddwyr yn gyfrinachol. (8 llythyren):

2 i lawr: Ynysu dyfeisiau terfynol heintiedig i atal llwythi bygythiad rhag lledaenu. (7 llythyren):

4 i lawr: Amgylchedd rhithwir ynysig a ddefnyddir i ddadansoddi ffeiliau maleisus yn ddiogel. (10 llythyren):

6 i lawr: Maleiswedd sy'n amgryptio storfa'r system ac yn mynnu taliad am yr allwedd. (10 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.

U S T E L J B R A B C P X L K

Y K X T K D Q O M J C D I N N

D K Q P G M M O Q R Y S T T G

D N C S Q O H T S B F W D S Z

E Y V C Z C W K F K Y H Z B D

W D N D Q E X I P C N U B L A

M Y Z N D F K T Y A G D O W D

O W F H I F D R S D U Q M C E

S M I R Z Y S F B I Q V F H A

N A Q O N L P T I F X Q K T R

A U S D N P Y B W F F S X Y W

R J A R Z R Y Y E E L G I W M

R J M L T E O H D I Q Q H O Z

A O V G U N B Y D L R Y B D H

L Z G J O P N W C M Z Y G Y O

RHESTR GEIRIAU GEIRFA

CEFFYLPREN

RANSOMWEDD

YSBIWEDD

ROOTKIT

BLWCHTYWOD

CYFYNGU

MWYDYN

DIFFEIL

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. CEFFYLPREN

B. RANSOMWEDD

C. YSBIWEDD

D. ROOTKIT

E. BLWCHTYWOD

F. CYFYNGU

G. MWYDYN

H. DIFFEIL

DIFFINIADAU A MEYSYDD PARU

1. Maleiswedd lechwraidd sy'n cuddio'n ddwfn yng nghnewyllyn y system i gadw rheolaeth weinyddol.

2. Ynysu dyfeisiau terfynol heintiedig i atal llwythi bygythiad rhag lledaenu.

3. Maleiswedd sy'n rhedeg yn uniongyrchol yn y RAM i osgoi cael ei chanfod gan sganwyr disg.

4. Maleiswedd sy'n ei dyblygu ei hun ac yn lledaenu ar draws rhwydweithiau heb weithred ddynol.

5. Maleiswedd sy'n amgryptio storfa'r system ac yn mynnu taliad am yr allwedd.

6. Rhaglen a gynlluniwyd i fonitro a chofnodi gweithgarwch a mewnbynnau defnyddwyr yn gyfrinachol.

7. Meddalwedd faleisus wedi'i chuddio fel rhaglen ddiniwed neu ddefnyddiol.

8. Amgylchedd rhithwir ynysig a ddefnyddir i ddadansoddi ffeiliau maleisus yn ddiogel.

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. EPLYECRNFF
2. IYDSDEWB
3. BTOYLHDCWW
4. NDYYMW
5. EMDASWORDN
6. IOKRTTO
7. CGNUYYF
8. IFLDIEF

Gweithgaredd Bonws: Meddwl yn Gyflym

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

1	Mannau i lawrlwytho apiau diogel			
2	Dyfeisiau y gellir eu hacio			
3	Pethau rydych chi'n gwneud copi wrth gefn ohonynt			
4	Arwyddion rhybudd mewn e-bost			
5	Arwyddion bod gan ffôn faleiswedd			
6	Mathau o faleiswedd rydych chi'n eu hadnabod			
7	Mathau o ffeiliau i fod yn ofalus â nhw			
8	Ffyrdd y mae maleiswedd yn cyrraedd cyfrifiadur personol			
9	Arferion diogel y gallwch eu dechrau heddiw			
10	Geiriau sy'n ymwneud â seiberddiogelwch			
11	Pethau i'w gwneud ar ôl gollyngiad data			
12	Rhesymau dros ddiweddaru meddalwedd			
13	Anifeiliaid neu gymeriadau ag enwau tebyg i faleiswedd			
14	Pethau y gall maleiswedd eu dwyn			
15	Pethau i'w gwneud os gwnaethoch glicio ar y ddolen anghywir			

Pwynt Gwirio 8: Astudiaethau Achos Seiberddiogelwch

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

ASTUDIAETH ACHOS 1: CYFYNGU AR LWYTH MEDDALWEDD PRIDWERTH MEWN MENTER

👷

Senario: Mae rhwydwaith ardal leol corfforaethol wedi cael ei dorri gan feddalwedd wystlo weithredol. Mae gweinyddion ffeiliau allweddol wedi dechrau dangos estyniadau ffeil gyda .locked. Sefydlwch bolisïau cyfyngu.

Cwestiwn Trafod: Disgrifiwch y camau cyfyngu yn fanwl, ac amlinellwch y protocol adfer data.

ASTUDIAETH ACHOS 2: CHWISTRELLU MALEISWEDD DDI-FFEIL I'R COF

👷

Senario: Mae dadansoddwr yn canfod patrymau sgriptio amheus sy'n gweithredu'n uniongyrchol yn RAM anweddol y system gan ddefnyddio offer gweinyddol safonol, ond nid oes unrhyw ffeiliau maleisus ar y ddisg.

Cwestiwn Trafod: Esboniwch y strategaeth dadansoddi cof, a nodwch offer i rwystro gweithredu heb ffeiliau.

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	14	6	25	4	4	23	3	8		12	23	25	20	8	9

7	25	4	1		13	15	14	9	20	18	15

25	13	4	4	25	7	9	1	4

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 maleiswedd?

Meddalwedd faleisus a gynlluniwyd gan actorion bygythiad i ddifrodi, herwgipio neu ddwyn data o ddyfeisiau a rhwydweithiau.

Q2: Beth yw'r gwahaniaeth rhwng feirws a mwydyn?

Mae angen gweithred ddynol (fel agor ffeil) ar firws i ledaenu, tra bo abwydyn yn lledaenu'n awtomatig ar draws rhwydweithiau.

Q3: Sut mae ceffyl Troea yn heintio cyfrifiadur?

Mae'n twyllo defnyddwyr drwy gymryd arno ei fod yn rhaglen ddiniwed neu ddiogel, gan guddio ei lwyth maleisus y tu mewn.

Q4: Beth yw meddalwedd wystlo?

Math o faleiswedd sy'n amgryptio ffeiliau ar y system darged, gan fynnu taliad ariannol yn gyfnewid am yr allwedd dadgryptio. [1]

Q5: Beth yw ysbïwedd?

Meddalwedd faleisus sy'n cofnodi trawiadau bysell, cyfrineiriau ac arferion pori defnyddwyr yn gyfrinachol i'w hanfon at ymosodwyr.

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

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

Q6: Beth yw ystyr blychau tywod (sandboxing)?

Rhedeg ffeiliau amheus mewn amgylchedd rhithwir diogel ac ynysig i arsylwi ar eu hymddygiad heb risg i systemau cynhyrchu.

Q7: Beth yw maleiswedd heb ffeiliau?

Maleiswedd sy'n rhedeg yn uniongyrchol yng nghof y system (RAM) gan ddefnyddio cyfleustodau cyfreithlon, gan osgoi ysgrifennu ffeiliau i'r ddisg er mwyn osgoi sganwyr sylfaenol.

Q8: Sut mae rootkit yn diogelu maleiswedd?

Mae'n cuddio prosesau a ffeiliau maleisus, yn aml drwy danseilio cnewyllyn y system weithredu, felly gall sganwyr gwrthfeirws eu methu.

Q9: Beth yw monitro ymddygiad deinamig?

Sganio gwrthfeirws sy'n monitro prosesau gweithredol mewn amser real i rwystro gweithredoedd sy'n nodweddiadol o faleiswedd, fel amgryptio ffeiliau mewn swmp.

Q10: Pam mae cyfyngu'n fater brys wrth ymateb i ddigwyddiad?

Mae ynysu dyfeisiau terfynol sydd wedi'u peryglu yn atal llwythi maleiswedd gweithredol rhag lledaenu i ddyfeisiau eraill ar y rhwydwaith.

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 datblygwyr maleiswedd yn osgoi sganwyr gwrthfeirws seiliedig ar lofnodion?

Maent yn defnyddio amlffurfedd, gan newid stwnsh a strwythur cod y ffeil gyda phob haint tra bo'r ymddygiad maleisus yn aros yr un fath.

Q2: Beth yw risg offer defnydd deuol mewn ymgyrchoedd maleiswedd?

Mae ymosodwyr yn defnyddio offer gweinyddol dilys (fel PowerShell neu Sysinternals) i ymdoddi i draffig rhwydwaith arferol, gan wneud canfod yn anodd.

Q3: Sut mae gwagio prosesau (process hollowing) yn gweithredu llwythi maleisus?

Mae'n lansio proses system ddilys mewn cyflwr ataliedig, yn disodli ei chod yn y cof â maleiswedd, ac yn ailddechrau'r gweithredu.

Q4: Beth yw rôl gweinydd Gorchymyn a Rheoli (C2)?

Gweinydd pell a weithredir gan hacwyr i anfon cyfarwyddiadau a llwythi tâl i faleiswedd sy'n rhedeg ar beiriannau sydd wedi'u cyfaddawdu.

Q5: Pam mae cofnodi trawiadau bysell (keylogging) yn anodd ei ganfod?

Mae cofnodwyr bysellau sylfaenol yn defnyddio ychydig iawn o adnoddau CPU ac yn cuddio eu prosesau y tu mewn i gyfleustodau dilys yng ngofod y defnyddiwr.

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

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

Q6: Sut mae cuddio cod (code obfuscation) yn oedi dadansoddi maleiswedd?

Mae'n amgryptio neu'n aildrefnu'r cod ffynhonnell, gan ei wneud yn annarllenadwy i offer dadansoddi a sganwyr diogelwch.

Q7: Beth yw swyddogaeth bootkit?

Rootkit sy'n heintio'r broses gychwyn (yr MBR, y sector cychwyn neu gadarnwedd UEFI), felly mae'n rhedeg cyn i'r system weithredu lwytho.

Q8: Sut mae sganio hewristig yn adnabod bygythiadau dim diwrnod?

Mae'n sganio am batrymau cod amheus a gorchmynion gweinyddol yn hytrach na chwilio am stwnsh cyfatebol mewn cronfa ddata.

Q9: Beth yw bygythiad herwgipio DLL?

Gorfodi rhaglen gyfreithlon i lwytho llyfrgell cyswllt deinamig (DLL) faleisus drwy ei gosod yn llwybr cyfeiriadur y rhaglen.

Q10: Sut mae piblinellau dadansoddi maleiswedd awtomataidd yn defnyddio rhithwiroli?

Maent yn rhedeg ffeiliau amheus ar draws peiriannau rhithwir sawl system weithredu, gan gynhyrchu logiau ymddygiad a ffeiliau PCAP rhwydwaith yn awtomatig.

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 ceffylau Troea yn parhau'n ddull heintio cyffredin oherwydd eu bod yn cuddio cod maleisus y tu mewn i raglenni sy'n edrych yn ddiniwed.

2. CIPOLWG AR DDIOGELWCH

Derbyniodd IC3 yr FBI dros 3,600 o gwynion am feddalwedd wystlo yn 2025, gyda cholledion a adroddwyd yn fwy na $32 miliwn. [3]

3. CIPOLWG AR DDIOGELWCH

Gall mwydod ledaenu'n gyflym ar draws rhwydweithiau drwy fanteisio ar wendidau protocol heb eu clytio, fel EternalBlue yn SMB.

4. CIPOLWG AR DDIOGELWCH

Mae maleiswedd ddi-ffeil yn anodd ei chanfod oherwydd ei bod yn rhedeg yn y cof drwy offer cyfreithlon ac yn gadael ychydig o olion ar y ddisg.

5. CIPOLWG AR DDIOGELWCH

Fel arfer mae blychau tywod dadansoddi yn dychwelyd i giplun glân ar ôl pob rhediad fel bod pob prawf yn dechrau o gyflwr hysbys.

6. CIPOLWG AR DDIOGELWCH

Gall rootkits addasu galwadau system y cnewyllyn, gan adrodd canlyniadau diagnostig ffug i sganwyr gwrth-faleiswedd.

7. MEWNWELEDIAD DIOGELWCH

Mae cuddio cod yn defnyddio cyfleustodau pacio i gywasgu a chuddio gwir strwythur llwyth deuaidd maleiswedd.

8. MEWNWELEDIAD DIOGELWCH

Mae maleiswedd amlffurf yn newid ei god, ac felly stwnsh ei ffeil, gyda phob copi newydd i osgoi gwiriadau llofnod.

9. MEWNWELEDIAD DIOGELWCH

Mae herwgipio DLL yn manteisio ar ffurfweddiadau trefn chwilio mewn systemau gweithredu safonol fel Windows.

10. CIPOLWG AR DDIOGELWCH

Mae gwerthwyr diogelwch yn canfod niferoedd enfawr o samplau maleiswedd newydd bob dydd, felly mae angen diweddaru llofnodion yn gyson.

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

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

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/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 **Cwestiwn 1** — **Ateb Cywir: A**

NODYN ADDYSGU

Beth yw nodwedd ddiffiniol ceffyl Troea? → Mae'n ymddangos fel meddalwedd ddilys i dwyllo defnyddwyr i'w rhedeg

2 **Cwestiwn 2** — **Ateb Cywir: A**

NODYN ADDYSGU

Pa fath o faleiswedd sy'n amgryptio ffeiliau ac yn mynnu taliad? → Nwyddau pridwerth

3 **Cwestiwn 3** — **Ateb Cywir: A**

NODYN ADDYSGU

Beth sy'n cynrychioli ysbïwedd? → Maleiswedd a gynlluniwyd i fonitro trawiadau bysell a gweithgareddau porwr defnyddwyr yn gyfrinachol

4 **Cwestiwn 4** — **Ateb Cywir: A**

NODYN ADDYSGU

Pam mae datblygwyr maleiswedd yn defnyddio rootkits? → I guddio prosesau gweithredol a ffeiliau maleisus rhag y system weithredu

5 **Cwestiwn 5** — **Ateb Cywir: A**

NODYN ADDYSGU

Beth yw ystyr blwch tywod wrth ddadansoddi maleiswedd? → Gweithredu ffeiliau amheus mewn claddgell rithwir ynysig i arsylwi ar eu hymddygiad yn ddiogel

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

6 **Cwestiwn 6** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: mae mwydod yn eu hatgynhyrchu eu hunain ac yn lledaenu ar draws rhwydweithiau heb unrhyw weithred gan ddefnyddiwr.

7 **Cwestiwn 7** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: nid yw meddalwedd hysbysebu (adware) bob amser yn ddiniwed; mae llawer ohoni'n tracio pori i dargedu hysbysebion.

8 **Cwestiwn 8** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Gwir: mae copïau wrth gefn glân all-lein yn adfer ffeiliau wedi'u hamgryptio heb dalu, er y gall data a ddygwyd ollwng o hyd.

9 **Cwestiwn 9** — **Ateb Cywir: Gau**

NODYN ADDYSGU

Gau: mae angen sampl hysbys ar sganwyr llofnodion, felly gall maleiswedd dim diwrnod newydd sbon lithro heibio iddynt.

10 **Cwestiwn 10** — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae maleiswedd ddi-ffeil yn rhedeg sgriptiau maleisus yng nghof y system, gan osgoi ysgrifennu ffeiliau i'r ddisg.

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

D 1. CEFFYL PREN	F 2. MEDDALWEDD WYSTLO	A 3. YSBÏWEDD	H 4. ROOTKIT
G 5. BLWCH TYWOD	C 6. CYFYNGU	E 7. MWYDYN	B 8. DI-FFEIL

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 CEFFYL PREN	2 RANSOMWEDD	3 YSBIWEDD	4 ROOTKIT
5 BLWCH TYWOD	6 CYFYNGU		

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 D – ROOTKIT	2 F – CYFYNGU	3 H – DIFFEIL	4 G – MWYDYN
5 B – RANSOMWEDD	6 C – YSBIWEDD	7 A – CEFFYLPREN	8 E – BLWCHTYWOD

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio CEFFYL PREN, MEDDALWEDD WYSTLO a YSBÏWEDD 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.

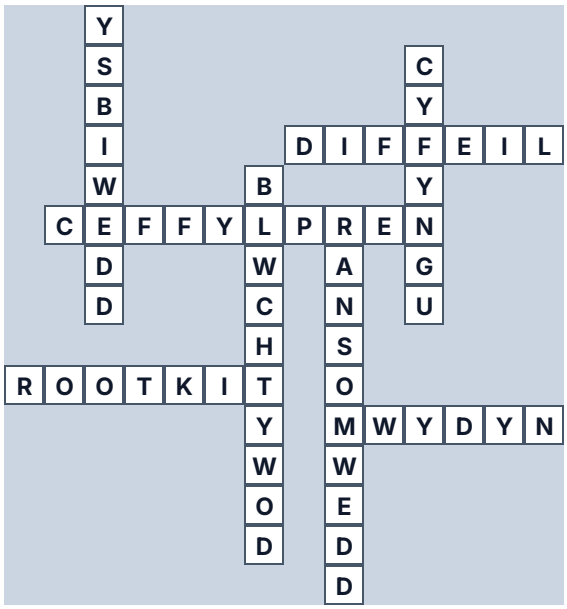
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

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

DATRYSIAD Y CROESAIR



CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

CLIWIAU AR DRAWS

3 ar draws: DIFFEIL Maleiswedd sy'n rhedeg yn uniongyrchol yn y RAM i osgoi cael ei chanfod gan sganwyr disg. (7 llythyren)

5 ar draws: CEFFYLPREN Meddalwedd faleisus wedi'i chuddio fel rhaglen ddiniwed neu ddefnyddiol. (10 llythyren)

7 ar draws: ROOTKIT Maleiswedd lechwraidd sy'n cuddio'n ddwfn yng nghnewyllyn y system i gadw rheolaeth weinyddol. (7 llythyren)

8 ar draws: MWYDYN Maleiswedd sy'n ei dyblygu ei hun ac yn lledaenu ar draws rhwydweithiau heb weithred ddynol. (6 llythyren)

CLIWIAU I LAWR

1 i lawr: YSBIWEDD Rhaglen a gynlluniwyd i fonitro a chofnodi gweithgarwch a mewnbynnau defnyddwyr yn gyfrinachol. (8 llythyren)

2 i lawr: CYFYNGU Ynysu dyfeisiau terfynol heintiedig i atal llwythi bygythiad rhag lledaenu. (7 llythyren)

4 i lawr: BLWCHTYWOD Amgylchedd rhithwir ynysig a ddefnyddir i ddadansoddi ffeiliau maleisus yn ddiogel. (10 llythyren)

6 i lawr: RANSOMWEDD Maleiswedd sy'n amgryptio storfa'r system ac yn mynnu taliad am yr allwedd. (10 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. E P L Y E C R N F F — **CEFFYLPREN**
2. I Y D S D E W B — **YSBIWEDD**
3. B T O Y L H D C W W — **BLWCHTYWOD**
4. N D Y Y M W — **MWYDYN**
5. E M D A S W O R D N — **RANSOMWEDD**
6. I O K R T T O — **ROOTKIT**
7. C G N U Y Y F — **CYFYNGU**
8. I F L D I E F — **DIFFEIL**

ALLWEDD HER Y SEIFFR CYFRINACHOL

"CANFYDDWCH LWYTHI GYDA MONITRO YMDDYGIAD"

Allwedd Atebion yr Astudiaethau Achos

A Astudiaeth Achos 1: Cyfyngu ar Lwyth Meddalwedd Pridwerth mewn Menter

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae nwyddau pridwerth gweithredol wedi torri i mewn i rwydwaith ardal leol corfforaethol. Mae gweinyddion ffeiliau allweddol wedi dechrau dangos estyniadau ffeil .locked. Sefydlwch bolisïau cyfyngu.
- Strategaeth a Datrysiad a Argymhellir: Datgysylltwch yr holl weinyddion yr effeithiwyd arnynt o'r rhwydwaith ardal leol. Terfynwch sesiynau gweinyddol gweithredol. Adferwch ffeiliau heb eu cyfaddawdu o system copïau wrth gefn all-lein ddiogel sydd wedi'i chloi rhag ysgrifennu.

B Astudiaeth Achos 2: Chwistrellu Maleiswedd Ddi-ffeil i'r Cof

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae dadansoddwr yn canfod patrymau sgriptio amheus yn gweithredu'n uniongyrchol yn RAM anweddol y system gan ddefnyddio offer gweinyddol safonol, ond nid oes unrhyw ffeiliau maleisus ar y ddisg.
- Strategaeth ac Ateb a Argymhellir: Ynyswch y pwyntiau terfyn yr effeithiwyd arnynt a chipiwch ddelwedd o'r cof yn gyntaf. Adolygwch logiau PowerShell a WMI, rhwystrwch sgriptiau heb eu cymeradwyo ag AppLocker, yna ailgychwynnwch i glirio'r llwyth.