Enw: _____ Dyddiad: _____ Sgôr: _____

Canllaw i'r VPN Mwyaf Diogel

Dadansoddiad technegol o ddyluniad VPN diogelwch uchel, gweinyddion cof anweddol RAM yn unig, diogelwch mynediad Zero Trust, amddiffynfeydd rhag gollyngiadau DNS preifat wedi'i amgryptio, a ffurfweddiadau WireGuard wedi'u harchwilio.

TROSOLWG DYSGU'R CANLLAW I'R VPN MWYAF DIOGEL

DYSGWR
STATWS MYFYRIWR
Llwybr Amddiffynnwr Rhwydwaith

DIOGEL
STATWS Y CYSYLLTIAD
Cysgodi pecynnau data

GWEITHREDOL
DIOGELU RHAG GOLLYNGIADAU
Diogelu rhag gollyngiadau DNS ac IPv6

Croeso! Mae'r pecyn gweithgareddau hwn yn eich tywys drwy safonau technegol VPNs hynod ddiogel. Byddwch yn archwilio caledwedd gweinyddion RAM yn unig, diogelwch mynediad Dim Ymddiriedaeth, datryswyr DNS preifat amgryptiedig a ffurfweddiadau WireGuard wedi'u harchwilio.

PWYNTIAU GWIRIO'R DAFLEN WAITH

- [ ] **Rhan 1-4: Meistroli ffurfweddiadau VPN a diogelwch rhwydwaith.**
- [ ] **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 VPNs Gorau VPN.com

URL: https://www.vpn.com/cy/vpn/vpn-mwyaf-diogel/

Eich Map Llwybr Dysgu'r VPN Mwyaf Diogel

- Dadansoddwch bensaernïaeth dechnegol a safonau amgryptio'r Canllaw VPN Mwyaf Diogel.
- Ffurfweddwch osodiadau'r cleient i atal gollyngiadau traffig IP, DNS a WebRTC.
- Cymharwch brotocolau twnelu perchnogol â gweithrediadau safonol.

CYFARWYDDIADAU'R CANLLAW I'R VPN MWYAF DIOGEL

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 galedwedd gweinyddion RAM-yn-unig a systemau Zero Trust. Gorffennwch gyda'r gweithgaredd bonws Meddwl yn Gyflym.

SEILWAITHAU RAM-YN-UNIG A RHWYDWEITHIAU ZERO TRUST (CYFLWYNIAD)

Mae VPN gwirioneddol ddiogel yn dibynnu ar fframwaith zero trust, gweinyddion RAM yn Unig i atal atafaelu disgiau rhag datgelu logiau, datryswyr DNS preifat wedi'u hamgryptio, a phrotocolau wedi'u harchwilio fel WireGuard. Mae'r rheolaethau cyfunol hyn yn amddiffyn asedau digidol gwerth uchel rhag bygythiadau rhyng-gipio.

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

Pwynt Gwirio 1: Her Amlddewis

1. **1. Pa bensaernïaeth sy'n hanfodol i sicrhau'r diogelwch uchaf mewn gweinyddion VPN modern?**
   - A) Seilwaith Gweinyddion RAM yn Unig
   - B) Storio ar Ddisg
   - C) Llwybro DNS Deinamig
   - D) Galluogi Anfon Pyrth Ymlaen

2. **2. Pa brotocol a argymhellir yn eang ar gyfer y ffurfweddiadau VPN mwyaf diogel a modern?**
   - A) WireGuard
   - B) PPTP
   - C) L2TP/IPSec
   - D) SSTP

3. **3. Pa fframwaith diogelwch sy'n gofyn am ddilysu pob cysylltiad yn barhaus heb eithriad?**
   - A) Pensaernïaeth Zero Trust
   - B) Waliau Tân Perimedr
   - C) Llwybro Deinamig
   - D) Allweddi Cyfrinachol a Rennir

4. **4. Beth yw prif rôl Diogelwch rhag Gollyngiadau DNS cleient VPN?**
   - A) Llwybro pob cais DNS drwy ddatryswyr preifat wedi'u hamgryptio
   - B) Cuddio pecynnau IP
   - C) Storio ymholiadau DNS mewn celc yn lleol
   - D) Analluogi Gweinyddion Enwau

5. **5. Sut mae llwybro Multi-Hop yn cynyddu diogelwch cyffredinol twnnel VPN?**
   - A) Yn llwybro data drwy ddau weinydd ar wahân yn olynol
   - B) Yn cynyddu cyflymder cywasgu
   - C) Yn amgryptio data â seiffrau diogelwch isel
   - D) Osgoi Waliau Tân

Pwynt Gwirio 2: Her Gwir neu Gau

6 Cwestiwn 6

6. Mae gweinyddion RAM-yn-Unig yn storio ffeiliau log mewn cof dros dro, sy'n cael ei sychu wrth ailgychwyn.

○ Gwir ○ Gau

7 Cwestiwn 7

7. Mae WireGuard yn defnyddio algorithmau cryptograffig modern sy'n llai agored i dagfeydd cyflymder.

○ Gwir ○ Gau

8 Cwestiwn 8

8. Mae kill switch VPN yn gweithio drwy flocio'r holl draffig rhwydwaith os bydd y twnnel yn gollwng.

○ Gwir ○ Gau

9 Cwestiwn 9

9. Nid yw archwiliadau annibynnol gan drydydd partïon yn berthnasol i ddilysu ymrwymiadau diogelwch.

○ Gwir ○ Gau

10 Cwestiwn 10

10. Mae modelau Dim Ymddiriedaeth yn tybio bod pob cysylltiad rhwydwaith mewnol yn ddiogel yn ddiofyn.

○ 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 gweinyddwyr yn gorfodi diogelwch drwy roi fframwaith _____ llym ar waith.

2. Mae llwybro pecynnau drwy sawl pwynt mynediad yn gofyn am ffurfweddiad _____ diogel.

3. Er mwyn atal gollyngiadau data o yriannau wedi'u dwyn, rydym yn defnyddio cynllun _____ .

4. Caiff herwgipio gan ISP ei liniaru drwy ffurfweddu nodweddion _____ brodorol.

5. I rwystro traffig pan fydd y cysylltiad yn methu, galluogwch y mecanwaith _____ .

6. Er mwyn lleihau logiau cronfa ddata sy'n cael eu storio, dewiswch ddarparwr sy'n gwbl _____ .

BANC GEIRIAU GEIRFA

AMGRYPTIO AML-NAID ARCHWILIEDIG DIM YMDDIRIED DIOGELU DNS
GWEINYDD RAM KILL SWITCH PROTOCOL

Ysgrifennwch eich atebion yma:

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

Pwynt Gwirio 4: Paru Cysyniadau VPN a Rhwydwaith

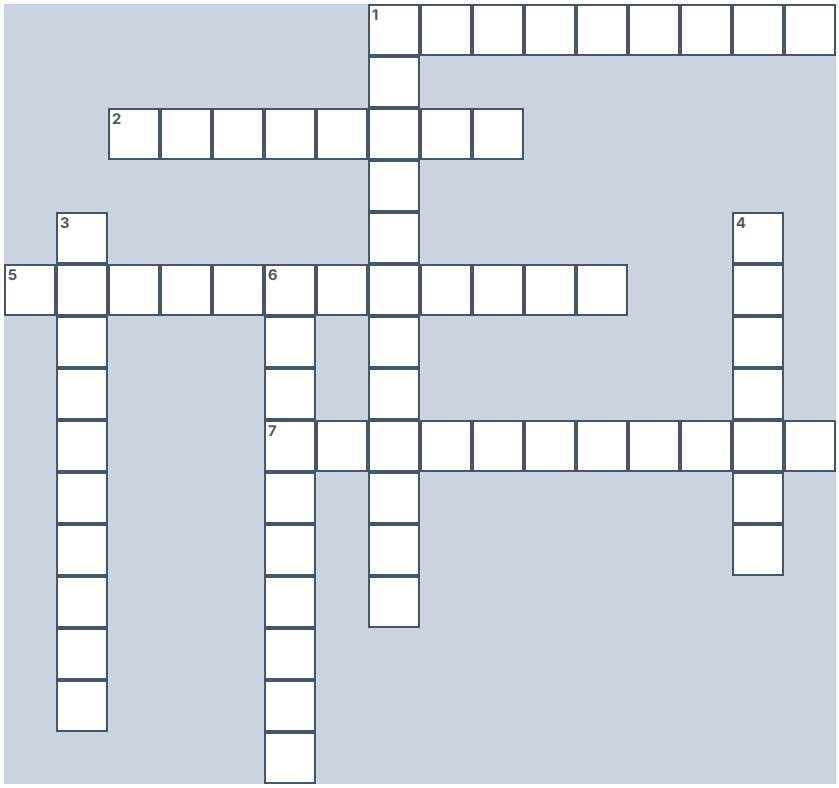
PARU DIFFINIADAU

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. Dim Ymddiriedaeth	A	Trefniant wedi'i archwilio'n annibynnol sy'n cadarnhau nad oes unrhyw logiau'n cael eu storio.
☐	2. Aml-Naid	B	Sgramblo llwythi data yn gryptograffig i'w diogelu wrth eu cludo.
☐	3. Gweinydd RAM-yn-Unig	C	Fframwaith diogelwch sy'n gofyn am ddilysu pob defnyddiwr yn barhaus.
☐	4. Diogelwch DNS	D	Set o reolau technegol sy'n pennu sut mae data'n cael ei becynnu a'i anfon.
☐	5. Kill Switch	E	Llwybro VPN rhaeadrol sy'n cadwyno dau nod gweinydd at ei gilydd.
☐	6. System wedi'i Harchwilio	F	Pensaernïaeth gweinydd sy'n defnyddio cof anweddol i storio llwythi data.
☐	7. Amgryptio	G	Gorfodi ymholiadau DNS preifat i ddiogelu chwiliadau gweinyddion enwau.
☐	8. Protocol	H	Mecanwaith diogelu rhag methiant sy'n rhwystro traffig os bydd y VPN yn methu.

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

1. Sgramblo cryptograffig llwythi data i'w diogelu wrth deithio (9)

2. Set o reolau technegol sy'n pennu sut mae data'n cael ei becynnu a'i anfon (8)

5. Fframwaith diogelwch sy'n gofyn am ddilysu pob defnyddiwr yn barhaus (12)

7. Pensaernïaeth gweinydd sy'n defnyddio cof anweddol i storio llwythi data (11)

CLIWIAU I LAWR

1. Gosodiad a arolygwyd yn annibynnol sy'n cadarnhau nad oes logiau'n cael eu storio (12)

3. Mecanwaith diogelwch sy'n rhwystro traffig os bydd y VPN yn methu (10)

4. Llwybro VPN rhaeadrol sy'n cadwyno dau nod gweinydd at ei gilydd (7)

6. Gorfodi ymholiadau DNS preifat i amddiffyn chwiliadau gweinyddion enwau (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

1 ar draws: Sgramblo cryptograffig llwythi data i'w diogelu wrth deithio (9 llythyren):

2 ar draws: Set o reolau technegol sy'n pennu sut mae data'n cael ei becynnu a'i anfon (8 llythyren):

5 ar draws: Fframwaith diogelwch sy'n gofyn am ddilysu pob defnyddiwr yn barhaus (12 llythyren):

7 ar draws: Pensaernïaeth gweinydd sy'n defnyddio cof anweddol i storio llwythi data (11 llythyren):

CLIWIAU I LAWR

1 i lawr: Gosodiad a arolygwyd yn annibynnol sy'n cadarnhau nad oes logiau'n cael eu storio (12 llythyren):

3 i lawr: Mecanwaith diogelwch sy'n rhwystro traffig os bydd y VPN yn methu (10 llythyren):

4 i lawr: Llwybro VPN rhaeadrol sy'n cadwyno dau nod gweinydd at ei gilydd (7 llythyren):

6 i lawr: Gorfodi ymholiadau DNS preifat i amddiffyn chwiliadau gweinyddion enwau (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.

G K E K Q N J D A F O K N D N

I C D H I B A I P R L P W T I

D Y F Y S G X O W H F R T N U

E K R D T S L G P L M S H K P

I H Y P L W U E N Y Q Q B G A

L L P M B L I L F I N Y B W A

I Z Z Y B N V U X M C F P E M

W W Q Q X H E D Y C W L F I L

H G H Z W C O N R J X X R N N

C K Z A N R Z S R M G S W Y A

R D I M Y M D D I R I E D D I

A G L A M G R Y P T I O W D D

J B K I L L S W I T C H Y R C

C Y O U Z O Z U T B H V P A X

C L O C O T O R P N M H P M X

RHESTR GEIRIAU GEIRFA

DIMYMDDIRIED AMLNAID GWEINYDDRAM DIOGELUDNS KILLSWITCH
ARCHWILIEDIG AMGRYPTIO PROTOCOL

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. DIMYMDDIRIED
B. AMLNAID
C. GWEINYDDRAM
D. DIOGELUDNS
E. KILLSWITCH
F. ARCHWILIEDIG
G. AMGRYPTIO
H. PROTOCOL

DIFFINIADAU A MEYSYDD PARU	
	1. Mecanwaith diogelwch sy'n rhwystro traffig os bydd y VPN yn methu.
	2. Gorfodi ymholiadau DNS preifat i amddiffyn chwiliadau gweinyddion enwau.
	3. Llwybro VPN rhaeadrol sy'n cadwyno dau nod gweinydd at ei gilydd.
	4. Set o reolau technegol sy'n pennu sut mae data'n cael ei becynnu a'i anfon.
	5. Sgramblo cryptograffig llwythi data i'w diogelu wrth deithio.
	6. Pensaernïaeth gweinydd sy'n defnyddio cof anweddol i storio llwythi data.
	7. Gosodiad a arolygwyd yn annibynnol sy'n cadarnhau nad oes logiau'n cael eu storio.
	8. Fframwaith diogelwch sy'n gofyn am ddilysu pob defnyddiwr yn barhaus.

Pwynt Gwirio 7: Her Geiriau Cymysg

Dad-sgramblwch y llythrennau isod i ddatgelu cysyniadau a thermau allweddol Rhwydwaith Preifat Rhithwir (VPN). Ysgrifennwch eich atebion yn y blychau mewnbwn a ddarperir.

1. RDIMIDIDEMDY
2. NMWGAYERDDI
3. KWCIISHLTL
4. YOIRTPAMG
5. ADNLAIM
6. NEGUDDILSO
7. IEWARLGDICIH
8. TROLPOCO

Gweithgaredd Bonws: Meddwl yn Gyflym

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

1	Cloeon neu allweddi rydych chi'n eu defnyddio bob dydd			
2	Pethau y gall VPN eu cuddio			
3	Pethau sy'n gwneud VPN yn ddiogel			
4	Mythau am VPNs			
5	Rhesymau dros ddefnyddio VPN wrth deithio			
6	Mannau diogel yn y byd go iawn			
7	Geiriau sy'n golygu 'wedi'i ddiogelu'			
8	Addewidion y mae darparwr VPN da yn eu gwneud			
9	Geiriau sy'n ymwneud â phreifatrwydd			
10	Mathau o archwiliad neu arolygiad			
11	Geiriau o'r daflen waith hon rydych chi am eu cofio			
12	Pethau y mae haciwr eisiau eu dwyn			
13	Ffyrdd o adnabod rhwydwaith Wi-Fi ffug			
14	Mannau lle byddech chi'n defnyddio VPN			
15	Pethau y gall eich darparwr rhyngrwyd eu gweld			

Pwynt Gwirio 8: Astudiaethau Achos VPN a Rhwydwaith

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

ASTUDIAETH ACHOS 1: CADARNHAU SEILWAITH MENTER



Senario: Mae banc corfforaethol yn ailddylunio topoleg ei fynediad o bell. Mae'n gofyn am bensaernïaeth zero trust sy'n cysylltu pob dyfais cleient â gweinyddion diogel.

Cwestiwn Trafod: Beth yw prif fantais micro-segmentu rhwydwaith o dan fodel VPN Zero Trust?

ASTUDIAETH ACHOS 2: MESURAU DIOGELU GWEINYDDION RAM YN UNIG



Senario: Mae darparwr VPN sy'n canolbwyntio ar ddiogelwch yn uwchraddio ei weinyddion i atal cipio gweinyddion ffisegol rhag datgelu hanes logiau defnyddwyr.

Cwestiwn Trafod: Esboniwch sut mae ffurfweddiadau caledwedd RAM-yn-unig yn atal tynnu data fforensig pan gaiff gweinyddion ffisegol eu cipio.

Pwynt Gwirio 9: Dadgryptio'r Seiffr

Mae peiriannydd rhwydwaith yn diogelu sianeli llwybro a thwneli cleientiaid. 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

22 16 14 1 21 4 9 15 7 5 12 25 14

7 23 1 18 3 8 15 4 1 19 5 4 1 21

4 9 7 9 4 15 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 VPN (Rhan A)

Adolygwch y cwestiynau a'r atebion mwyaf cyffredin am Rwydweithiau Preifat Rhithwir (VPNs) a thwnelu.

Q1: Beth sy'n gwneud VPN yn 'fwyaf diogel'?

Cyfuniad o Zero Trust, gweinyddion RAM yn unig a phrotocolau wedi'u harchwilio.

Q2: Beth yw gweinyddion RAM yn Unig?

Gweinyddion sy'n rhedeg mewn cof anweddol, wedi'u cynllunio i storio dim logiau ar ddisg.

Q3: Beth yw VPN Zero Trust?

Fframwaith sy'n dilysu pob cais am fynediad a phob cysylltiad yn barhaus.

Q4: Pam yr ystyrir bod WireGuard yn ddiogel?

Mae ganddo sylfaen cod fach sy'n hawdd ei harchwilio ac mae'n defnyddio seiffrau modern.

Q5: Sut mae VPNs diogel yn atal gollyngiadau DNS?

Drwy lwybro pob ymholiad drwy ddatryswyr DNS preifat wedi'u hamgryptio.

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

Adolygwch y cwestiynau a'r atebion mwyaf cyffredin am Rwydweithiau Preifat Rhithwir (VPNs) a thwnelu.

Q6: A oes angen archwiliadau ar VPN diogel?

Ie, mae archwiliadau annibynnol yn gwirio honiadau dim logiau a diogelwch y cod.

Q7: Beth yw rôl kill switch?

Mae'n atal traffig rhwydwaith ar unwaith os bydd y cysylltiad VPN yn torri.

Q8: Pa amgryptio sy'n cael ei ddefnyddio mewn VPNs diogel?

AES-256 a ChaCha20 yw safonau'r diwydiant ar gyfer amgryptio.

Q9: A yw llwybro Multi-Hop yn ddiogel?

Ie, mae'n cysylltu dau weinydd neu fwy mewn cadwyn i atal dadansoddi traffig.

Q10: Sut mae awdurdodaeth alltraeth yn helpu?

Gall gyfyngu ar ba gyfreithiau sy'n berthnasol, ond nid yw'n cynnig imiwnedd llwyr.

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

Archwilio agweddau technegol uwch ar brotocolau twnelu VPN, integreiddio cleientiaid symudol, a defnyddio mewn mentrau.

Q1: Sut mae gweinyddion RAM yn unig yn atal y risg o atafaelu data?

Gan eu bod yn rhedeg mewn RAM, mae tynnu'r plwg yn dileu'r data a gedwir yn y cof.

Q2: Sut mae Zero Trust yn disodli diogelwch perimedr safonol?

Mae'n trin pob cleient fel un gelyniaethus, gan ofyn am ddilysu parhaus.

Q3: Beth sy'n gwneud cod WireGuard yn haws i'w archwilio?

Mae ei god Linux yn llai na 4,000 o linellau, yn llawer llai na phentyrrau VPN arferol. [4]

Q4: Sut mae DNSSEC yn diogelu ymholiadau DNS?

Mae'n llofnodi cofnodion DNS fel y gall datryswyr ganfod atebion ffug neu rai yr ymyrrwyd â nhw.

Q5: Sut mae Multi-Hop yn cymhlethu cydberthynas traffig?

Drwy wahanu cyfeiriadau IP i mewn ac allan ar draws gwahanol ddarparwyr lletya.

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

Archwilio agweddau technegol uwch ar brotocolau twnelu VPN, integreiddio cleientiaid symudol, a defnyddio mewn mentrau.

Q6: Pam mae awdurdodaethau Five Eyes yn beryglus i VPNs?

Mae aelod-wladwriaethau'n rhannu cudd-wybodaeth a gallant ddefnyddio gorchmynion cyfreithiol i geisio data defnyddwyr.

Q7: Sut mae kill switch yn cael ei weithredu ar lefel y cnewyllyn?

Mae'n defnyddio rheolau wal dân y system (fel iptables neu WFP) i rwystro traffig sy'n gadael.

Q8: Beth yw cyfrinachedd ymlaen mewn ysgwyd llaw VPN?

Mae'n cynhyrchu allweddi sesiwn unigryw fel na ellir dadgryptio sesiynau blaenorol.

Q9: Sut mae VPNs diogel yn lliniaru gollyngiadau WebRTC?

Drwy rwystro ceisiadau WebRTC neu eu llwybro drwy'r twnnel.

Q10: Sut mae archwiliadau annibynnol yn sicrhau cydymffurfiaeth preifatrwydd?

Mae archwilwyr yn cynnal profion treiddio ac yn archwilio ffurfweddiadau gweinyddion.

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

Adolygwch ffeithiau o'r byd go iawn am gyflymderau amgryptio VPN, archwiliadau protocol, cysylltedd symudol, a gweithio o bell mewn mentrau.

1. CIPOLWG AR VPN

Mae gweinyddion RAM-yn-unig yn llwytho eu system weithredu i'r cof wrth gychwyn, felly does dim yn aros ar ddisg ar ôl ailgychwyn.

2. CIPOLWG AR VPN

Mae WireGuard yn defnyddio fframwaith Noise gyda Curve25519, ChaCha20, Poly1305, BLAKE2s a HKDF. [3]

3. CIPOLWG AR VPN

Mae Dim Ymddiriedaeth yn caniatáu mynediad fesul adnodd ac nid yw'n rhoi unrhyw ymddiriedaeth ymhlyg ar sail lleoliad rhwydwaith (NIST SP 800-207). [1]

4. CIPOLWG AR VPN

Mae cynghrair cudd-wybodaeth y Five Eyes yn cynnwys yr Unol Daleithiau, y DU, Canada, Awstralia a Seland Newydd.

5. CIPOLWG AR VPN

Mae gollyngiadau WebRTC yn digwydd pan fydd porwyr yn datgelu cyfeiriad IP cyhoeddus go iawn y cleient drwy ymholiadau STUN.

6. CIPOLWG AR VPN

Mae perfect forward secrecy (PFS) yn sicrhau nad yw peryglu allwedd hirdymor yn datgelu allweddi sesiynau blaenorol. [3]

7. MEWNWELEDIAD VPN

Mae Cure53, cwmni diogelwch o Berlin, wedi cyhoeddi archwiliadau o sawl darparwr VPN.

8. MEWNWELEDIAD VPN

Mae gollyngiadau DNS yn digwydd pan fydd ymholiadau DNS yn osgoi twnnel y VPN ac yn mynd i weinyddion enwau'r ISP lleol.

9. MEWNWELEDIAD VPN

Mae angen pŵer trydan cyson ar sglodion RAM anweddol i gadw data, ac maent yn colli eu cynnwys pan gânt eu diffodd.

10. CIPOLWG AR VPN

Mae systemau Dim Ymddiriedaeth menter yn gorfodi gwiriadau ystum dyfais cyn caniatáu cysylltu ag adnoddau diogel. [1]

Cyfeiriadau a Ffynonellau Technegol

Mae'r canllaw astudio a'r posau rhyngweithiol wedi'u llunio o safonau technegol, manylebau a fframweithiau rheoleiddio byd-eang.

CYFEIRIADAU YSGOLHEIGAIDD A DIWYDIANT

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[6] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

Allwedd Atebion: Pwynt Gwirio 1 – Amlddewis

1 **Gweinydd RAM-yn-Unig** RAM-YN-UNIG — **Ateb Cywir: A**

NODYN ADDYSGU

Nid yw gweinyddion RAM-yn-Unig yn storio unrhyw logiau ar ddisg, ac maent yn sychu data wrth ailgychwyn. Dyfyniad: Most Secure VPN.

2 **Cwestiwn 2** — **Ateb Cywir: A**

NODYN ADDYSGU

Mae WireGuard yn cyfuno sylfaen god fach y gellir ei harchwilio â seiffrau modern.

3 **Model Dim Ymddiriedaeth** DIM YMDDIRIEDAETH — **Ateb Cywir: A**

NODYN ADDYSGU

Mae modelau Dim Ymddiriedaeth yn gwirio cydymffurfiaeth dyfeisiau'n barhaus cyn caniatáu mynediad. Ffynhonnell: Most Secure VPN.

4 **Diogelwch DNS** DIOGELU DNS — **Ateb Cywir: A**

NODYN ADDYSGU

Mae Diogelu rhag Gollyngiadau DNS yn llwybro ymholiadau chwilio drwy ddatryswyr preifat. Ffynhonnell: Most Secure VPN.

5 **Twneli Aml-Naid** AML-HOP — **Ateb Cywir: A**

NODYN ADDYSGU

Mae llwybro Aml-hop yn cadwyno dau nod gweinydd ar wahân yn olynol. Ffynhonnell: Most Secure VPN.

Allwedd Atebion: Pwynt Gwirio 2 – Gwir neu Gau

6 **Gweinydd RAM-yn-Unig** RAM-YN-UNIG — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Nid yw caledwedd gweinyddion RAM-yn-Unig yn ysgrifennu unrhyw ddata i ddisg, ac mae'n sychu wrth ailgychwyn. Dyfyniad: Most Secure VPN.

7 **Cyflymder WireGuard** WIREGUARD — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae WireGuard yn defnyddio cryptograffeg fodern sy'n osgoi tagfeydd prosesu. Ffynhonnell: Most Secure VPN.

8 **Kill Switch** SWITS DIOGELU RHAG METHIANT — **Ateb Cywir: Gwir**

NODYN ADDYSGU

Mae kill switch yn blocio'r holl draffig os bydd cysylltiad y VPN yn gollwng. Ffynhonnell: Most Secure VPN.

9 **Archwiliadau Trydydd Parti** ARCHWILIADAU'N HANFODOL — **Ateb Cywir: Gau**

NODYN ADDYSGU

Mae archwiliadau trydydd parti yn hanfodol i ddilysu honiadau preifatrwydd cwmnïau. Dyfyniad: Most Secure VPN.

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

NODYN ADDYSGU

Nid yw Zero Trust yn rhoi unrhyw ymddiriedaeth ymhlyg ar sail lleoliad yn y rhwydwaith. [1]

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

C 1. Dim Ymddiriedaeth	E 2. Aml-Naid	F 3. Gweinydd RAM-yn-Unig	G 4. Diogelwch DNS
H 5. Kill Switch	A 6. System wedi'i Harchwilio	B 7. Amgryptio	D 8. Protocol

PWYNT GWIRIO 3: ALLWEDD TERMAU ALLWEDDOL

1 DIM YMDDIRIED	2 AML-NAID	3 GWEINYDD RAM	4 DIOGELU DNS
5 KILL SWITCH	6 ARCHWILIEDIG		

PWYNT GWIRIO 6, DEWIS ARALL: ALLWEDD PARU GEIRFA

1 E – KILLSWITCH	2 D – DIOGELUDNS	3 B – AMLNAID	4 H – PROTOCOL
5 G – AMGRYPTIO	6 C – GWEINYDDRAM	7 F – ARCHWILIEDIG	8 A – DIMYMDDIRIED

NODIADAU TRAFOD I ATHRAWON

Termau Allweddol:
Gwiriwch fod myfyrwyr yn gallu esbonio Dim Ymddiriedaeth, Aml-Naid a Gweinydd RAM-yn-Unig 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.

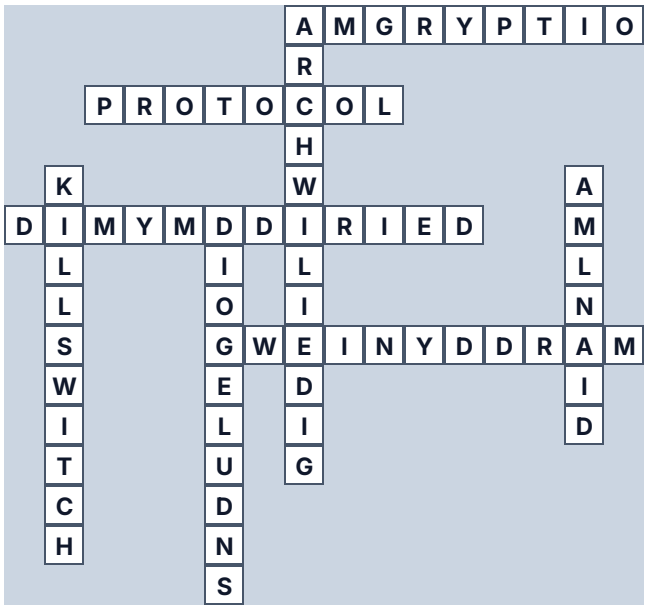
Gwerthuso Ffynonellau:
Gofynnwch i fyfyrwyr wirio o leiaf un honiad yn erbyn cyfeiriadau'r daflen waith, a thrafodwch pam y gall ffigurau, prisiau a rheolau newid dros amser.

Allweddi Posau a Nodiadau i Athrawon

DATRYSIAD Y CHWILAIR

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

DATRYSIAD Y CROESAIR



CANLLAW I ATHRAWON AR GYFER ATEBION Y CROESAIR

CLIWIAU AR DRAWS

1 ar draws: AMGRYPTIO Sgramblo cryptograffig llwythi data i'w diogelu wrth deithio (9 llythyren)

2 ar draws: PROTOCOL Set o reolau technegol sy'n pennu sut mae data'n cael ei becynnu a'i anfon (8 llythyren)

5 ar draws: DIMYMDDIRIED Fframwaith diogelwch sy'n gofyn am ddilysu pob defnyddiwr yn barhaus (12 llythyren)

7 ar draws: GWEINYDDRAM Pensaernïaeth gweinydd sy'n defnyddio cof anweddol i storio llwythi data (11 llythyren)

CLIWIAU I LAWR

1 i lawr: ARCHWILIEDIG Gosodiad a arolygwyd yn annibynnol sy'n cadarnhau nad oes logiau'n cael eu storio (12 llythyren)

3 i lawr: KILLSWITCH Mecanwaith diogelwch sy'n rhwystro traffig os bydd y VPN yn methu (10 llythyren)

4 i lawr: AMLNAID Llwybro VPN rhaeadrol sy'n cadwyno dau nod gweinydd at ei gilydd (7 llythyren)

6 i lawr: DIOGELUDNS Gorfodi ymholiadau DNS preifat i amddiffyn chwiliadau gweinyddion enwau (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. RDIMIDIDEMDY — **DIMYMDDIRIED**
2. NMWGAYERDDI — **GWEINYDDRAM**
3. KWCIISHLTL — **KILLSWITCH**
4. YOIRTPAMG — **AMGRYPTIO**
5. ADNLAIM — **AMLNAID**
6. NEGUDDILSO — **DIOGELUDNS**
7. IEWARLGDICIH — **ARCHWILIEDIG**
8. TROLPOCO — **PROTOCOL**

ALLWEDD HER Y SEIFFR CYFRINACHOL

"VPNAU DIOGEL YN GWARCHOD ASEDAU DIGIDOL"

Allwedd Atebion yr Astudiaethau Achos

A ASTUDIAETH ACHOS 1: CADARNHAU SEILWAITH MENTER

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae banc corfforaethol yn ailgynllunio topoleg ei fynediad o bell. Mae angen pensaernïaeth dim ymddiriedaeth arno sy'n cysylltu pob dyfais cleient â gweinyddion diogel.
- Strategaeth ac Ateb a Argymhellir: Canllawiau Marcio: Esboniwch fod micro-segmentu yn cyfyngu mynediad i adnoddau penodol, gan atal bygythiadau rhag symud yn ochrol os caiff dyfais ei chyfaddawdu.

B ASTUDIAETH ACHOS 2: MESURAU DIOGELU GWEINYDDION RAM YN UNIG

Datrysiad i Athrawon

CANLLAW MARCIO

Dylai atebion myfyrwyr gwmpasu'r pwyntiau canlynol:

- Dadansoddi Senario: Mae darparwr VPN sy'n canolbwyntio ar ddiogelwch yn uwchraddio ei weinyddion i atal atafaelu gweinyddion ffisegol rhag datgelu hanes logiau defnyddwyr.
- Strategaeth ac Ateb a Argymhellir: Canllawiau Marcio: Dylid nodi nad oes gan weinyddion RAM-yn-unig storfa ddisg ffisegol. Mae colli pŵer yn dileu'r holl ddata dros dro yn y cof anweddol yn awtomatig.