Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

Ασφάλεια Surfshark

Εξέταση των λειτουργιών ασφάλειας του Surfshark, συμπεριλαμβανομένων του αποκλεισμού διαφημίσεων CleanWeb, της δυναμικής δρομολόγησης MultiHop, της αρχιτεκτονικής SDN Nexus, του στόλου διακομιστών μόνο με RAM και της λειτουργίας Camouflage.

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ: ΑΣΦΑΛΕΙΑ SURFSHARK

ΜΑΘΗΤΗΣ

ΙΔΙΟΤΗΤΑ ΦΟΙΤΗΤΗ

Διαδρομή Network Defender

ΑΣΦΑΛΕΣ

ΚΑΤΑΣΤΑΣΗ ΣΥΝΔΕΣΗΣ

Θωράκιση πακέτων δεδομένων

ΕΝΕΡΓΟ

ΠΡΟΣΤΑΣΙΑ ΔΙΑΡΡΟΩΝ

Προστασία από διαρροές DNS και IPv6

Καλώς ήρθες! Αυτό το φυλλάδιο δραστηριοτήτων σε καθοδηγεί στην αρχιτεκτονική ασφαλείας της Surfshark. Θα εξερευνήσεις το υλικό διακομιστών αποκλειστικά RAM, τη δυναμική εναλλαγή IP του Nexus SDN, τα προγράμματα αποκλεισμού διαφημίσεων CleanWeb και τη δρομολόγηση MultiHop.

ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ ΤΟΥ ΦΥΛΛΟΥ ΕΡΓΑΣΙΑΣ

- ☐ **Μέρη 1-4: Κατάκτησε τις διαμορφώσεις VPN και ασφάλειας δικτύου.**
- ☐ **Μέρη 5-7: Λύσε γρίφους σταυρολέξου και αναζήτησης λέξεων.**
- ☐ **Μέρη 8-9: Λύσε μελέτες περίπτωσης και πρόκληση κρυπτογραφημένου μηνύματος.**
- ☐ **Μέρος 10: Εξέτασε τις σελίδες συχνών ερωτήσεων βασικού και προχωρημένου επιπέδου.**
- ☐ **Μέρος 11: Εξερεύνησε 10 ενδιαφέροντα πραγματικά στοιχεία.**
- ☐ **Μπόνους: η πρόκληση Σκέψου γρήγορα.**

Άνοιξε τον Οδηγό του VPN.com για τα καλύτερα VPN

URL: https://www.vpn.com/el/vpn/surfshark/asfalia/

Η πορεία μάθησής σου: ασφάλεια Surfshark

- Ανάλυσε την τεχνική αρχιτεκτονική και τους κανόνες διαμόρφωσης του Surfshark (ασφάλεια).
- Ρύθμισε τις παραμέτρους του πελάτη ώστε να αποτρέπονται οι διαρροές κίνησης IP, DNS και WebRTC.
- Σύγκρινε την προσαρμοσμένη τιμολόγηση, τη δοκιμή και τα χαρακτηριστικά απόδοσης με τα τυπικά μοντέλα.

ΟΔΗΓΙΕΣ ΟΔΗΓΟΥ ΑΣΦΑΛΕΙΑΣ SURFSHARK

Απάντησε στις ερωτήσεις πολλαπλής επιλογής και σωστού/λάθους, συμπλήρωσε τα κενά των προτάσεων με την τράπεζα λέξεων, αντιστοίχισε ορισμούς και λύσε το σταυρόλεξο και τον γρίφο αναζήτησης λέξεων. Εφάρμοσε τις γνώσεις σου στην υποδομή μόνο RAM, στο Nexus SDN και στο CleanWeb. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΣΤΟΛΟΣ ΔΙΑΚΟΜΙΣΤΩΝ ΜΟΝΟ ΜΕ RAM, NEXUS SDN ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΗ CLEANWEB (ΕΙΣΑΓΩΓΗ)

Η Surfshark προστατεύει το απόρρητο των χρηστών με στόλο διακομιστών αποκλειστικά RAM, δικτύωση καθορισμένη από λογισμικό Nexus με IP Rotator, αποκλεισμό διαφημίσεων CleanWeb και δυναμικές διαδρομές κρυπτογράφησης MultiHop.

ΔΙΑΒΑΣΕ ΠΡΟΣΕΚΤΙΚΑ ΚΑΘΕ ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ ΚΑΙ ΕΠΙΛΕΞΕ Η ΓΡΑΨΕ ΤΗ ΣΩΣΤΗ ΑΠΑΝΤΗΣΗ.

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **1. Ποιο είναι το όνομα του ενσωματωμένου αποκλεισμού διαφημίσεων και κακόβουλου λογισμικού της Surfshark;**
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. **2. Ποια αρχιτεκτονική υλικού χρησιμοποιεί η Surfshark σε όλους τους διακομιστές της;**
   - A) Σκληροί δίσκοι
   - B) 100% μόνο RAM
   - C) Οπτική αποθήκευση
   - D) Μαγνητική ταινία

3. **3. Ποιο χαρακτηριστικό δρομολογεί την κίνηση μέσω δύο διαφορετικών διακομιστών VPN;**
   - A) Bypasser
   - B) MultiHop (Διπλό VPN)
   - C) Δίκτυο Nexus
   - D) Στατική IP

4. **4. Ποιο χαρακτηριστικό συσκότισης (obfuscation) μεταμφιέζει την κίνηση VPN σε κανονικά δεδομένα ιστού;**
   - A) Kill Switch
   - B) Λειτουργία καμουφλάζ
   - C) CleanWeb 2.0
   - D) Split Tunnel

5. **5. Ποια είναι η λειτουργία του εργαλείου Surfshark Bypasser;**
   - A) Speed Booster
   - B) Split Tunneling
   - C) Διαχειριστής κωδικών πρόσβασης
   - D) Επιλυτής DNS

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Οι διακομιστές μόνο με RAM διαγράφουν όλα τα λειτουργικά δεδομένα αμέσως μετά την επανεκκίνηση του διακομιστή.

○ Σωστό ○ Λάθος

7 Ερώτηση 7

7. Η λειτουργία Camouflage εμποδίζει τους ISP να εντοπίσουν ότι χρησιμοποιείς VPN.

○ Σωστό ○ Λάθος

8 Ερώτηση 8

8. Το CleanWeb 2.0 λειτουργεί μέσα σε επεκτάσεις προγράμματος περιήγησης για να αποκλείει αναδυόμενα παράθυρα συγκατάθεσης για cookies.

○ Σωστό ○ Λάθος

9 Ερώτηση 9

9. Η Surfshark διατηρεί προσωρινές χρονοσφραγίδες συνδέσεων και αρχεία καταγραφής χρήσης εύρους ζώνης.

○ Σωστό ○ Λάθος

10 Ερώτηση 10

10. Το δίκτυο Nexus εναλλάσσει περιοδικά τις διευθύνσεις IP των χρηστών χωρίς αποσύνδεση.

○ Σωστό ○ Λάθος

Σημείο ελέγχου 3: Συμπλήρωση βασικών όρων

Διάβασε κάθε πρόταση παρακάτω και συμπλήρωσε το κενό με τον σωστό όρο από την Τράπεζα Λέξεων.

1. Οι ενοχλητικές διαφημίσεις web, τα σενάρια παρακολούθησης και οι σύνδεσμοι phishing μπλοκάρονται από φίλτρα _____ .

2. Η δραστηριότητα του χρήστη δεν αφήνει εγκληματολογικά ίχνη επειδή οι διακομιστές λειτουργούν με τεχνολογία _____ .

3. Η δρομολόγηση δεδομένων μέσω δύο ξεχωριστών κρυπτογραφημένων βημάτων διακομιστή γίνεται με σήραγγες _____ .

4. Για να κρύψουν τη χρήση VPN από τους παρόχους διαδικτύου, οι χρήστες ενεργοποιούν τη λειτουργία _____ .

5. Η παράκαμψη του VPN από τραπεζικές εφαρμογές διαχειρίζεται από τις ρυθμίσεις _____ .

6. Η αρχιτεκτονική SDN επόμενης γενιάς που συνδέει το σύνολο των διακομιστών είναι το σύστημα _____ .

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΔΙΑΚΟΠΤΗΣ ΔΡΟΜΟΛΟΓΗΣΗ ΕΝΑΛΛΑΓΗ ΜΟΝΟ ΜΝΗΜΗ ΠΑΡΑΚΑΜΨΗ
ΦΙΛΤΡΟ CAMOUFLAGE NEXUS

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών VPN και δικτύου

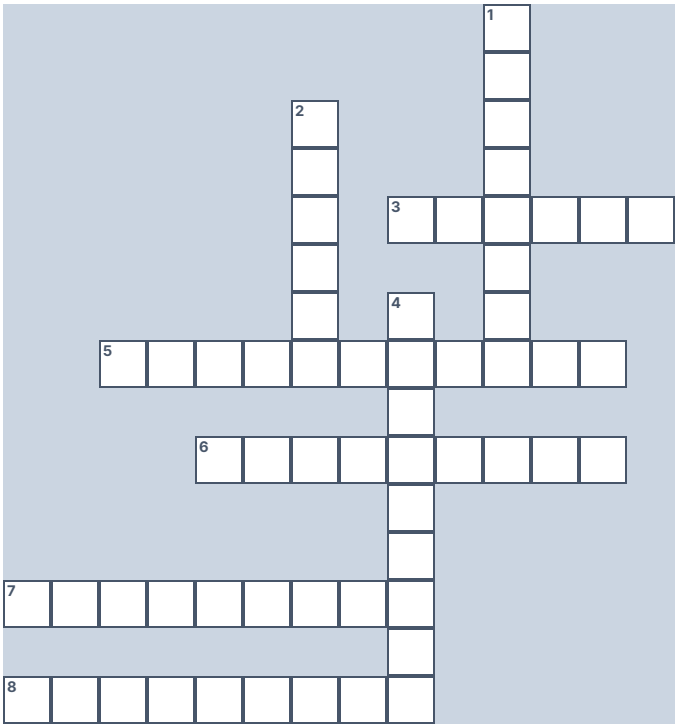
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

Αντιστοίχισε κάθε όρο λεξιλογίου στα αριστερά με τον σωστό ορισμό του στα δεξιά, γράφοντας το αντίστοιχο γράμμα (A-H) στο πλαίσιο εισαγωγής.

☐	1. ΦΙΛΤΡΟ	A	Μια αυτόματη λειτουργία ασφαλείας που αποκλείει την κίνηση δικτύου όταν πέφτει το VPN.
☐	2. ΜΟΝΟ ΜΝΗΜΗ	B	Λειτουργία split-tunneling που επιτρέπει σε επιλεγμένες εφαρμογές να παρακάμπτουν το VPN.
☐	3. ΔΡΟΜΟΛΟΓΗΣΗ	C	Ένα προηγμένο φίλτρο που αποκλείει διαφημίσεις, κακόβουλο λογισμικό και banner συγκατάθεσης cookie.
☐	4. ΛΑΘΡΑΙΑ ΣΥΝΔΕΣΗ	D	Υλικό διακομιστών πτητικής μνήμης που διαγράφει όλα τα δεδομένα σε κάθε κύκλο ενεργοποίησης και απενεργοποίησης.
☐	5. ΠΑΡΑΚΑΜΠΤΗΣ	E	Μια λειτουργία που αλλάζει τακτικά την εξωτερική διεύθυνση IP σου χωρίς να διακόπτει τις σήραγγες.
☐	6. ΔΙΑΚΟΠΤΗΣ	F	Τεχνολογία συσκότισης που κρύβει τις υπογραφές VPN ώστε να μοιάζουν με κανονική κίνηση HTTPS.
☐	7. NEXUS NET	G	Μια λειτουργία δρομολόγησης διπλού VPN που κρυπτογραφεί την κίνηση μέσω δύο διαφορετικών κόμβων διακομιστών.
☐	8. ΠΕΡΙΣΤΡΕΦΟΜΕΝΗ	H	Ένα ιδιοκτησιακό δίκτυο καθορισμένο από λογισμικό που συνδέει όλους τους διακομιστές σε ένα ενιαίο πλέγμα.

Σημείο ελέγχου 5: Σταυρόλεξο

Λύσε το σταυρόλεξο πληκτρολογώντας γράμματα στα ενεργά λευκά κουτιά. Οι αριθμοί αντιστοιχούν στις οδηγίες παρακάτω.



ΟΡΙΖΟΝΤΙΑ

3. Προηγμένος αποκλεισμός διαφημίσεων, κακόβουλου λογισμικού και μηνυμάτων συγκατάθεσης για cookie (6)

5. Λειτουργία διπλού VPN που περνά την κίνηση μέσω δύο διαφορετικών κόμβων διακομιστή (11)

6. Αυτόματη λειτουργία ασφαλείας που μπλοκάρει την κίνηση του δικτύου όταν πέσει το VPN (9)

7. Τεχνολογία συσκότισης που κρύβει τις υπογραφές VPN ώστε να μοιάζουν με κανονική κίνηση HTTPS (9)

8. Λειτουργία διαχωρισμού σήραγγας που επιτρέπει σε επιλεγμένες εφαρμογές να αγνοούν το VPN (9)

ΚΑΘΕΤΑ

1. Λειτουργία που αλλάζει τακτικά την εξωτερική σου διεύθυνση IP χωρίς να διακόπτει τις σήραγγες (8)

2. Ιδιόκτητη υποδομή ορισμένη από λογισμικό που συνδέει όλους τους διακομιστές σε ενιαίο πλέγμα (6)

4. Υλικό διακομιστή με πτητική μνήμη που σβήνει όλα τα δεδομένα σε κάθε επανεκκίνηση (9)

Σημείο ελέγχου 5, εναλλακτικά: Προσβάσιμες ενδείξεις σταυρολέξου

Οι χρήστες αναγνώστη οθόνης και πληκτρολογίου μπορούν να πληκτρολογήσουν τις απαντήσεις του σταυρολέξου απευθείας στα πεδία κειμένου παρακάτω.

ΟΡΙΖΟΝΤΙΑ

3 οριζόντια: Προηγμένος αποκλεισμός διαφημίσεων, κακόβουλου λογισμικού και μηνυμάτων συγκατάθεσης για cookie (6 γράμματα):

5 οριζόντια: Λειτουργία διπλού VPN που περνά την κίνηση μέσω δύο διαφορετικών κόμβων διακομιστή (11 γράμματα):

6 οριζόντια: Αυτόματη λειτουργία ασφαλείας που μπλοκάρει την κίνηση του δικτύου όταν πέσει το VPN (9 γράμματα):

7 οριζόντια: Τεχνολογία συσκότισης που κρύβει τις υπογραφές VPN ώστε να μοιάζουν με κανονική κίνηση HTTPS (9 γράμματα):

8 οριζόντια: Λειτουργία διαχωρισμού σήραγγας που επιτρέπει σε επιλεγμένες εφαρμογές να αγνοούν το VPN (9 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Λειτουργία που αλλάζει τακτικά την εξωτερική σου διεύθυνση IP χωρίς να διακόπτει τις σήραγγες (8 γράμματα):

2 κάθετα: Ιδιόκτητη υποδομή ορισμένη από λογισμικό που συνδέει όλους τους διακομιστές σε ενιαίο πλέγμα (6 γράμματα):

4 κάθετα: Υλικό διακομιστή με πτητική μνήμη που σβήνει όλα τα δεδομένα σε κάθε επανεκκίνηση (9 γράμματα):

Σημείο ελέγχου 6: Αναζήτηση κρυμμένων λέξεων

Βρες τους 8 βασικούς όρους λεξιλογίου που κρύβονται στο παρακάτω πλέγμα. Οι λέξεις μπορεί να είναι οριζόντιες, κάθετες ή διαγώνιες.

Γ	Ρ	Ο	Θ	Ζ	Ν	Π	Δ	Μ	Ο	Χ	Π	Ξ	Γ	Τ
Σ	Σ	Ρ	Ε	Λ	Ι	Β	Ι	Α	Β	Ε	Γ	Ξ	Ψ	Λ
Κ	Ψ	Τ	Λ	Χ	Τ	Κ	Α	Δ	Π	Ν	Μ	Ι	Δ	Θ
Η	Ν	Λ	Ν	Κ	Π	Ο	Κ	Η	Μ	Α	Μ	Π	Ρ	Σ
Μ	Τ	Ι	Τ	Η	Δ	Γ	Ο	Σ	Ο	Λ	Ξ	Θ	Σ	Ρ
Η	Β	Φ	Φ	Δ	Ρ	Σ	Π	Ω	Υ	Λ	Γ	Ω	Υ	Φ
Ν	Ζ	Κ	Η	Ω	Ο	Δ	Τ	Π	Ν	Α	Δ	Π	Γ	Χ
Μ	Ο	Γ	Τ	Β	Μ	Α	Η	Α	Ω	Γ	Ν	Δ	Κ	Λ
Ο	Α	Δ	Ξ	Δ	Ο	Ε	Σ	Ρ	Η	Η	Θ	Δ	Α	Ρ
Ν	Π	Μ	Ε	Θ	Λ	Δ	Ρ	Α	Ω	Σ	Ε	Π	Λ	Υ
Ο	Ε	Α	Α	Π	Ο	Ι	Ξ	Κ	Ν	Ο	Τ	Χ	Υ	Π
Μ	Κ	Ρ	Τ	Ρ	Γ	Κ	Γ	Α	Ν	Ψ	Β	Ζ	Ψ	Ρ
Χ	Φ	Ι	Α	Ρ	Η	Τ	Ω	Μ	Ψ	Ψ	Λ	Ζ	Η	Θ
Μ	Π	Κ	Μ	Μ	Σ	Υ	Σ	Ψ	Ξ	Η	Ο	Π	Η	Ω
Α	Ξ	Υ	Ζ	Υ	Η	Ο	Β	Η	Ψ	Ρ	Ψ	Β	Η	Μ

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΦΙΛΤΡΟ ΜΟΝΟΜΝΗΜΗ ΔΡΟΜΟΛΟΓΗΣΗ ΣΥΓΚΑΛΥΨΗ ΠΑΡΑΚΑΜΨΗ ΔΙΑΚΟΠΤΗΣ ΔΙΚΤΥΟ ΕΝΑΛΛΑΓΗ

Σημείο ελέγχου 6, εναλλακτικά: Προσβάσιμη αντιστοίχιση λεξιλογίου

Αντιστοίχισε καθέναν από τους 8 όρους λεξιλογίου του Word Search με τον σωστό ορισμό του, γράφοντας το γράμμα (A-H) στο κενό.

ΟΡΟΙ ΛΕΞΙΛΟΓΙΟΥ

A. ΦΙΛΤΡΟ

B. ΜΟΝΟΜΝΗΜΗ

C. ΔΡΟΜΟΛΟΓΗΣΗ

D. ΣΥΓΚΑΛΥΨΗ

E. ΠΑΡΑΚΑΜΨΗ

F. ΔΙΑΚΟΠΤΗΣ

G. ΔΙΚΤΥΟ

H. ΕΝΑΛΛΑΓΗ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

1. Τεχνολογία συσκότισης που κρύβει τις υπογραφές VPN ώστε να μοιάζουν με κανονική κίνηση HTTPS.

2. Αυτόματη λειτουργία ασφαλείας που μπλοκάρει την κίνηση του δικτύου όταν πέσει το VPN.

3. Προηγμένος αποκλεισμός διαφημίσεων, κακόβουλου λογισμικού και μηνυμάτων συγκατάθεσης για cookie.

4. Λειτουργία διαχωρισμού σήραγγας που επιτρέπει σε επιλεγμένες εφαρμογές να αγνοούν το VPN.

5. Υλικό διακομιστή με πτητική μνήμη που σβήνει όλα τα δεδομένα σε κάθε επανεκκίνηση.

6. Λειτουργία που αλλάζει τακτικά την εξωτερική σου διεύθυνση IP χωρίς να διακόπτει τις σήραγγες.

7. Λειτουργία διπλού VPN που περνά την κίνηση μέσω δύο διαφορετικών κόμβων διακομιστή.

8. Ιδιόκτητη υποδομή ορισμένη από λογισμικό που συνδέει όλους τους διακομιστές σε ενιαίο πλέγμα.

Σημείο ελέγχου 7: Πρόκληση ανακατεμένων λέξεων

Αποκωδικοποίησε τα γράμματα παρακάτω για να αποκαλύψεις βασικές έννοιες και όρους των εικονικών ιδιωτικών δικτύων (VPN). Γράψε τις απαντήσεις σου στα διαθέσιμα πλαίσια εισαγωγής.

1. ΛΦΤΡΟΙ
2. ΟΗΡΔΣΛΟΗΓΟΜ
3. ΠΑΚΑΜΗΑΨΡ
4. ΟΤΚΥΔΙ
5. ΗΜΟΗΝΟΜΜΝ
6. ΨΚΥΥΛΣΑΗΓ
7. ΠΔΗΣΤΚΙΟΑ
8. ΛΝΛΗΕΓΑΑ

Δραστηριότητα μπόνους: Σκέψου γρήγορα

3 ΑΠΑΝΤΗΣΕΙΣ ΓΙΑ ΚΑΘΕ ΚΑΤΗΓΟΡΙΑ. ΚΕΡΔΙΖΕΙ ΟΠΟΙΟΣ ΣΥΜΠΛΗΡΩΣΕΙ ΠΡΩΤΟΣ ΤΗ ΛΙΣΤΑ.

1	Λειτουργίες ασφάλειας στο Surfshark			
2	Ενδείξεις ότι η σύνδεση VPN σου είναι αργή			
3	Πρωτόκολλα VPN που γνωρίζεις			
4	Πράγματα που προστατεύει η κρυπτογράφηση			
5	Απειλές στο δημόσιο Wi-Fi			
6	Χώρες γνωστές για τους ισχυρούς νόμους απορρήτου			
7	Τρόποι να φτιάξεις έναν ισχυρό κωδικό πρόσβασης			
8	Συσκευές στις οποίες θα εγκαθιστούσες το Surfshark			
9	Ερωτήσεις προς την υποστήριξη πελατών του Surfshark			
10	Ρυθμίσεις που ενεργοποιείς για επιπλέον ασφάλεια			
11	Πράγματα που το Surfshark μπορεί να κρύψει από το δίκτυό σου			
12	Τύποι διαρροών VPN			
13	Δεδομένα που ένα VPN δεν πρέπει να αποθηκεύει ποτέ			
14	Λέξεις που περιγράφουν μια καλή εφαρμογή VPN			
15	Πράγματα που μπορεί να ελέγξει ένας έλεγχος (audit)			

Σημείο ελέγχου 8: Μελέτες περίπτωσης VPN και δικτύου

Εφάρμοσε τις έννοιες που έμαθες για να λύσεις τα παρακάτω σενάρια πραγματικού κόσμου.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΠΑΡΑΚΑΜΨΗ ΦΙΛΤΡΩΝ CAMPUS ΚΑΙ ΧΩΡΟΥ ΕΡΓΑΣΙΑΣ



Σενάριο: Ένας φοιτητής διαπιστώνει ότι το Wi-Fi της πανεπιστημιούπολής του μπλοκάρει όλες τις τυπικές θύρες OpenVPN και WireGuard.

Ερώτηση συζήτησης: Ποια λειτουργία του Surfshark επιτρέπει στον φοιτητή να συνδεθεί χωρίς να εντοπιστεί από τους διαχειριστές του δικτύου;

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΔΗΜΟΣΙΟΓΡΑΦΙΚΗ ΕΡΕΥΝΑ ΥΨΗΛΟΥ ΚΙΝΔΥΝΟΥ



Σενάριο: Ένας ερευνητής δημοσιογράφος χρειάζεται επιπλέον προστασία από την παρακολούθηση ενώ ερευνά ευαίσθητα εταιρικά αρχεία.

Ερώτηση συζήτησης: Πώς προσφέρει το Dynamic MultiHop ανώτερο απόρρητο σε σύγκριση με τη δρομολόγηση μέσω ενός διακομιστή;

Σημείο ελέγχου 9: Αποκρυπτογράφησε τον κώδικα

Ένας μηχανικός δικτύων ασφαλίζει τα κανάλια δρομολόγησης και τις σήραγγες πελατών. Χρησιμοποίησε το παρακάτω κλειδί Γράμμα-Αριθμός για να αποκρυπτογραφήσεις το μήνυμα γράφοντας τα αντίστοιχα γράμματα στα κενά.

ΚΛΕΙΔΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΓΡΑΜΜΑΤΟΣ ΣΕ ΑΡΙΘΜΟ

Α=1 Β=2 Γ=3 Δ=4 Ε=5 Ζ=6 Η=7 Θ=8

Ι=9 Κ=10 Λ=11 Μ=12 Ν=13 Ξ=14 Ο=15 Π=16

Ρ=17 Σ=18 Τ=19 Υ=20 Φ=21 Χ=22 Ψ=23 Ω=24

5	13	1	11	11	1	3	7		4	9	5	20	8	20	13	18	5	24	13
5	13	9	18	22	20	5	9		19	15		1	16	15	17	17	7	19	15

Αποκρυπτογραφημένο μήνυμα:

ΣΥΜΒΟΥΛΗ: ΚΑΘΕ ΑΡΙΘΜΟΣ ΕΚΠΡΟΣΩΠΕΙ ΤΗ ΘΕΣΗ ΤΟΥ ΓΡΑΜΜΑΤΟΣ ΣΤΟ ΑΛΦΑΒΗΤΟ (Π.Χ. 1 = Α, 2 = Β, 24 = Ω).

Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – βασικό επίπεδο (Μέρος Α)

Εξέτασε τις πιο συχνές ερωτήσεις και απαντήσεις για τα εικονικά ιδιωτικά δίκτυα (VPN) και τη σηραγγοποίηση.

Q1: Τι είναι το Surfshark CleanWeb;

Το CleanWeb είναι μια ενσωματωμένη λειτουργία ασφαλείας που αποκλείει διαφημίσεις, ιχνηλάτες, κακόβουλο λογισμικό και ιστότοπους ηλεκτρονικού ψαρέματος.

Q2: Τι είναι οι διακομιστές μόνο RAM;

Οι διακομιστές μόνο με RAM λειτουργούν με πτητική μνήμη, που σημαίνει ότι τα δεδομένα που βρίσκονται στη μνήμη διαγράφονται κάθε φορά που επανεκκινούνται οι διακομιστές.

Q3: Τι είναι το Surfshark MultiHop;

Το MultiHop (Double VPN) δρομολογεί και κρυπτογραφεί τη σύνδεσή σου στο διαδίκτυο μέσω δύο διαφορετικών τοποθεσιών διακομιστών.

Q4: Πώς λειτουργεί η Camouflage Mode;

Η λειτουργία Camouflage αποκρύπτει την κίνηση VPN, ώστε ο ISP σου να μην μπορεί να καταλάβει ότι χρησιμοποιείς VPN.

Q5: Τι είναι η λειτουργία Bypasser;

Το Bypasser είναι το εργαλείο split tunneling της Surfshark που επιτρέπει σε συγκεκριμένες εφαρμογές ή ιστότοπους να παρακάμπτουν το VPN.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – βασικό επίπεδο (Μέρος Β)

Εξέτασε τις πιο συχνές ερωτήσεις και απαντήσεις για τα εικονικά ιδιωτικά δίκτυα (VPN) και τη σηραγγοποίηση.

Q6: Διαθέτει η Surfshark Kill Switch;

Ναι, το Kill Switch σε αποσυνδέει από το διαδίκτυο αν το VPN πέσει απροσδόκητα.

Q7: Ποιο πρότυπο κρυπτογράφησης χρησιμοποιεί η Surfshark;

Η Surfshark χρησιμοποιεί AES-256-GCM και ChaCha20, καθώς και AEGIS-256X2 στο νέο της πρωτόκολλο Dausos.

Q8: Έχει ελεγχθεί η πολιτική no-logs της Surfshark;

Ναι, η Deloitte επαλήθευσε την πολιτική μη καταγραφής της Surfshark το 2023 και ξανά το 2025.

Q9: Τι είναι το Surfshark Nexus;

Το Nexus είναι μια προηγμένη αρχιτεκτονική SDN που συνδέει όλους τους διακομιστές σε ένα ενιαίο δίκτυο για ομαλότερη δρομολόγηση.

Q10: Τι είναι η λειτουργία IP Rotator;

Το IP Rotator αλλάζει αυτόματα τη διεύθυνση IP σου κάθε λίγα λεπτά χωρίς να διακόπτει τη συνεδρία VPN.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – προχωρημένο επίπεδο (Μέρος C)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πρωτοκόλλων τούνελ VPN, της ενσωμάτωσης προγραμμάτων πελάτη σε κινητά και της επιχειρησιακής ανάπτυξης.

Q1: Σε τι διαφέρει το Dynamic MultiHop από το παραδοσιακό Double VPN;

Το Dynamic MultiHop σου επιτρέπει να προσαρμόσεις οποιονδήποτε συνδυασμό διακομιστών εισόδου και εξόδου σε όλο τον κόσμο.

Q2: Λειτουργεί το CleanWeb 2.0 σε επεκτάσεις προγράμματος περιήγησης;

Ναι, το CleanWeb 2.0 μπλοκάρει διαφημίσεις βίντεο, αναδυόμενα παράθυρα συναίνεσης cookies και πλαίσια ειδοποιήσεων μέσα στο Chrome/Firefox.

Q3: Τι είναι το Alternative ID στη σουίτα ασφαλείας;

Το Alternative ID δημιουργεί μοναδικά προσωπικά ψευδώνυμα, διευθύνσεις email και μάσκες τηλεφώνου.

Q4: Πώς αποτρέπει η Surfshark τις διαρροές DNS;

Η Surfshark δρομολογεί όλα τα αιτήματα ονομάτων τομέα μέσω των δικών της ιδιωτικών διακομιστών DNS σε κάθε κόμβο.

Q5: Υποστηρίζει η Surfshark κρυπτογράφηση ChaCha20 στα κινητά;

Ναι, το WireGuard σε Android και iOS χρησιμοποιεί ChaCha20-Poly1305 για ανώτερη αποδοτικότητα στα κινητά.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – προχωρημένο επίπεδο (Μέρος D)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πρωτοκόλλων τούνελ VPN, της ενσωμάτωσης προγραμμάτων πελάτη σε κινητά και της επιχειρησιακής ανάπτυξης.

Q6: Τι είναι η λειτουργία NoBorders στη Surfshark;

Το NoBorders εντοπίζει αυτόματα περιοριστικά περιβάλλοντα δικτύου και παρέχει ειδικούς διακομιστές.

Q7: Ποιος πραγματοποίησε τους ελέγχους ασφαλείας στις επεκτάσεις προγράμματος περιήγησης της Surfshark;

Η ανεξάρτητη εταιρεία κυβερνοασφάλειας Cure53 ολοκλήρωσε ελέγχους σε επεκτάσεις προγραμμάτων περιήγησης και συστήματα διακομιστών.

Q8: Πώς προστατεύει η Surfshark από διαρροές IPv6;

Η Surfshark δρομολογεί την κίνηση IPv6 με ασφάλεια ή την περιορίζει με ασφάλεια ώστε να αποτραπεί οποιαδήποτε μη κρυπτογραφημένη διαρροή.

Q9: Πού βρίσκεται η νομική δικαιοδοσία της Surfshark;

Η Surfshark λειτουργεί υπό το δίκαιο της Ολλανδίας, τηρώντας τα αυστηρά ευρωπαϊκά πρότυπα απορρήτου του GDPR.

Q10: Υποστηρίζει το Surfshark έλεγχο ταυτότητας δύο παραγόντων (2FA);

Ναι, και το Surfshark One προσθέτει κλείδωμα 2FA ώστε μόνο εσύ να μπορείς να αλλάζεις τις ρυθμίσεις των χαρακτηριστικών.

Μέρος 11: 10 πραγματικά στοιχεία και διαπιστώσεις για τα VPN

Εξέτασε πραγματικά στοιχεία για τις ταχύτητες κρυπτογράφησης VPN, τους ελέγχους πρωτοκόλλων, την κινητή συνδεσιμότητα και την απομακρυσμένη εργασία σε επιχειρήσεις.

1. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

1. Η Surfshark αναφέρει ότι ολόκληρο το δίκτυο των 4.500+ διακομιστών της λειτουργεί με υλικό μόνο RAM, χωρίς δίσκους, με πτητική μνήμη.

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

2. Η εταιρεία της μεγάλης τετράδας Deloitte επαλήθευσε την πολιτική μη καταγραφής της Surfshark το 2023 και ξανά τον Νοέμβριο του 2025.

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

3. Η ιδιόκτητη αρχιτεκτονική Nexus συνδέει όλους τους παγκόσμιους διακομιστές σε ένα δυναμικό δίκτυο καθοριζόμενο από λογισμικό.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

4. Το Rotating IP αλλάζει τη διεύθυνση IP σου περίπου κάθε πέντε λεπτά χωρίς να διακόπτεται η σύνδεση VPN.

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

5. Το CleanWeb 2.0 αποκλείει απευθείας στα προγράμματα περιήγησης ενοχλητικά αναδυόμενα παράθυρα συναίνεσης για cookies και διαφημίσεις βίντεο.

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

6. Το Dynamic MultiHop επιτρέπει στους χρήστες να δημιουργούν προσαρμοσμένες διαδρομές κρυπτογράφησης δύο διακομιστών σε 100 χώρες.

7. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

7. Η Λειτουργία Παραλλαγής αφαιρεί τις υπογραφές κεφαλίδων του VPN, ώστε η κίνηση να μην ξεχωρίζει από την κανονική HTTPS.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

8. Το Alternative ID δημιουργεί ψευδώνυμα μίας χρήσης και μάσκες email για την προστασία των χρηστών από διαρροές βάσεων δεδομένων.

9. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

9. Η Surfshark εφαρμόζει συμμετρική κρυπτογράφηση AES-256-GCM μαζί με ChaCha20 στα πρωτόκολλα WireGuard.

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

10. Η λειτουργία NoBorders ενεργοποιείται αυτόματα σε περιορισμένα δίκτυα για να παρέχει ανθεκτική πρόσβαση μέσω τούνελ.

Τεχνικές αναφορές και πηγές

Ο οδηγός μελέτης και τα διαδραστικά παζλ έχουν συνταχθεί από παγκόσμια τεχνικά πρότυπα, προδιαγραφές και ρυθμιστικά πλαίσια.

ΑΚΑΔΗΜΑΪΚΕΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 **Ενσωματωμένο εργαλείο αποκλεισμού περιεχομένου** ΑΜΥΝΑ ΕΝΑΝΤΙ ΔΙΑΦΗΜΙΣΕΩΝ ΚΑΙ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ **Σωστή απάντηση: Β**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το CleanWeb είναι το ενσωματωμένο φίλτρο ασφαλείας του Surfshark που αποκλείει διαφημίσεις, τομείς ιχνηλατών, ιστότοπους ηλεκτρονικού ψαρέματος και κακόβουλα σενάρια URL σε επίπεδο δικτύου. Παραπομπή: Προδιαγραφές ασφαλείας CleanWeb.

2 **Υποδομή 100% μόνο RAM** ΑΡΧΙΤΕΚΤΟΝΙΚΗ RAM **Σωστή απάντηση: Β**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η Surfshark λειτουργεί διακομιστές αποκλειστικά RAM, επομένως τα δεδομένα που φυλάσσονται στη μνήμη του διακομιστή διαγράφονται όταν ο διακομιστής απενεργοποιείται ή επανεκκινείται. Παραπομπή: Cure53 Infrastructure Audit.

3 **Διπλό τούνελ MultiHop** VPN MULTIHOP **Σωστή απάντηση: Β**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το MultiHop (Double VPN) κρυπτογραφεί την κίνηση μέσω δύο διακριτών κόμβων διακομιστών σε διαφορετικές χώρες για να αποτρέψει επιθέσεις συσχέτισης κίνησης. Παραπομπή: Surfshark MultiHop Guide.

4 **Απόκρυψη (obfuscation) με τη λειτουργία Camouflage** ΣΥΣΚΟΤΙΣΗ **Σωστή απάντηση: Β**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η λειτουργία Camouflage τροποποιεί τις κεφαλίδες πακέτων του OpenVPN ώστε να μεταμφιέζει την κίνηση VPN σε τυπική κίνηση HTTPS, παρακάμπτοντας τους αποκλεισμούς περιοριστικών τειχών προστασίας. Παραπομπή: Λευκή βίβλος Surfshark Stealth.

5 **Split tunneling Bypasser** ΔΙΑΧΩΡΙΣΜΟΣ ΣΗΡΑΓΓΑΣ **Σωστή απάντηση: Β**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το Bypasser είναι το εργαλείο split tunneling της Surfshark που επιτρέπει στους χρήστες να επιλέγουν συγκεκριμένες εφαρμογές ή ιστότοπους που θα δρομολογούνται απευθείας μέσω της κανονικής σύνδεσης του ISP τους. Παραπομπή: Surfshark Client Features.

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 **Διαγραφή δεδομένων πτητικής μνήμης** ΑΣΦΑΛΕΙΑ ΔΙΑΚΟΜΙΣΤΗ Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι διακομιστές μόνο με RAM δεν αποθηκεύουν κανένα δεδομένο σε μόνιμους σκληρούς δίσκους· η επανεκκίνηση του υλικού διαγράφει αμέσως όλη τη λειτουργική μνήμη. Πηγή: RAM Server Architecture.

7 **Απόκρυψη του ISP με τη λειτουργία Camouflage** ΑΠΟΚΡΥΨΗ ΚΙΝΗΣΗΣ Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η λειτουργία Camouflage αφαιρεί τις υπογραφές του πρωτοκόλλου OpenVPN, εμποδίζοντας τους ISP να εντοπίσουν ότι ο χρήστης είναι συνδεδεμένος σε σήραγγα VPN. Παραπομπή: Οδηγός επιθεώρησης πακέτων σε βάθος.

8 **Επεκτάσεις προγράμματος περιήγησης CleanWeb 2.0** ΕΠΕΚΤΑΣΗ ΠΡΟΓΡΑΜΜΑΤΟΣ ΠΕΡΙΗΓΗΣΗΣ Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το CleanWeb 2.0 λειτουργεί μέσα σε επεκτάσεις προγράμματος περιήγησης και αποκλείει σε πραγματικό χρόνο αναδυόμενα παράθυρα συγκατάθεσης για cookies, διαφημίσεις βίντεο και κακόβουλα σενάρια ανακατεύθυνσης. Παραπομπή: Σημειώσεις έκδοσης CleanWeb 2.0.

9 **Μηδενική διατήρηση αρχείων σύνδεσης** ΠΟΛΙΤΙΚΗ ΜΗ ΚΑΤΑΓΡΑΦΗΣ Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η Surfshark τηρεί αυστηρή πολιτική μηδενικής καταγραφής με ανεξάρτητο έλεγχο, χωρίς καταγραφή διευθύνσεων IP, χρονοσφραγίδων συνδέσεων ή εύρους ζώνης. Παραπομπή: Deloitte No-Logs Audit.

10 **Δυναμική εναλλαγή IP Nexus** ΔΙΚΤΥΟ NEXUS Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το δίκτυο καθορισμένο από λογισμικό Surfshark Nexus εναλλάσσει δυναμικά τις διευθύνσεις IP των χρηστών κάθε λίγα λεπτά χωρίς να διακόπτει την ενεργή σύνδεση VPN. Παραπομπή: Surfshark Nexus Architecture.

Λύσεις λεξιλογίου και κριτήρια βαθμολόγησης

Κριτήρια βαθμολόγησης για τον εκπαιδευτικό: Δώσε 1 μονάδα για κάθε σωστή αντιστοίχιση (σύνολο 8 μονάδες) και για κάθε όρο περιεχομένου (σύνολο 6 μονάδες).

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 4: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΕΝΝΟΙΩΝ

C 1. ΦΙΛΤΡΟ	D 2. ΜΟΝΟ ΜΝΗΜΗ	G 3. ΔΡΟΜΟΛΟΓΗΣΗ	F 4. ΛΑΘΡΑΙΑ ΣΥΝΔΕΣΗ
B 5. ΠΑΡΑΚΑΜΠΤΗΣ	A 6. ΔΙΑΚΟΠΤΗΣ	H 7. NEXUS NET	E 8. ΠΕΡΙΣΤΡΕΦΟΜΕΝΗ

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΦΙΛΤΡΟ	2 ΜΟΝΟ ΜΝΗΜΗ	3 ΔΡΟΜΟΛΟΓΗΣΗ	4 CAMOUFLAGE
5 ΠΑΡΑΚΑΜΨΗ	6 NEXUS		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 D – ΣΥΓΚΑΛΥΨΗ	2 F – ΔΙΑΚΟΠΤΗΣ	3 A – ΦΙΛΤΡΟ	4 E – ΠΑΡΑΚΑΜΨΗ
5 B – ΜΟΝΟΜΝΗΜΗ	6 H – ΕΝΑΛΛΑΓΗ	7 C – ΔΡΟΜΟΛΟΓΗΣΗ	8 G – ΔΙΚΤΥΟ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους ΦΙΛΤΡΟ, ΜΟΝΟ ΜΝΗΜΗ και ΔΡΟΜΟΛΟΓΗΣΗ και να δώσουν ένα παράδειγμα για τον καθένα.

Μελέτες περίπτωσης:
Ζήτησε από τους μαθητές να στηρίζουν τις προτάσεις τους σε στοιχεία του φύλλου εργασίας και όχι σε υποθέσεις.

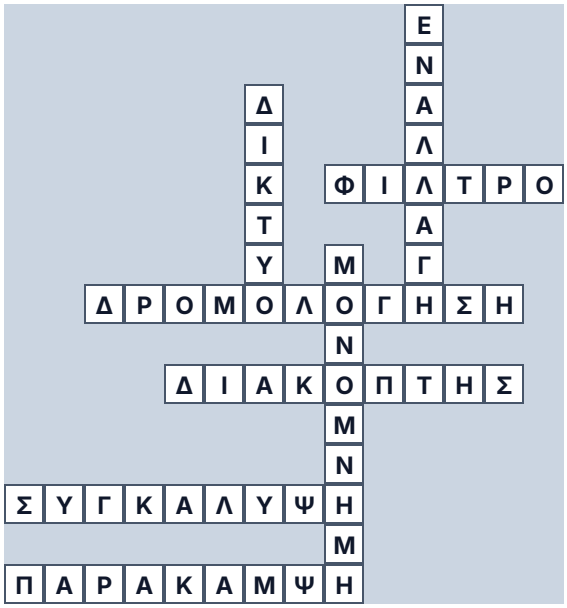
Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ

Γ	Ρ	Ο	Θ	Ζ	Ν	Π	Δ	Μ	Ο	Χ	Π	Ξ	Γ	Τ
Σ	Σ	Ρ	Ε	Λ	Ι	Β	Ι	Α	Β	Ε	Γ	Ξ	Ψ	Λ
Κ	Ψ	Τ	Λ	Χ	Τ	Κ	Α	Δ	Π	Ν	Μ	Ι	Δ	Θ
Η	Ν	Λ	Ν	Κ	Π	Ο	Κ	Η	Μ	Α	Μ	Π	Ρ	Σ
Μ	Τ	Ι	Τ	Η	Δ	Γ	Ο	Σ	Ο	Λ	Ξ	Θ	Σ	Ρ
Η	Β	Φ	Φ	Δ	Ρ	Σ	Π	Ω	Υ	Λ	Γ	Ω	Υ	Φ
Ν	Ζ	Κ	Η	Ω	Ο	Δ	Τ	Π	Ν	Α	Δ	Π	Γ	Χ
Μ	Ο	Γ	Τ	Β	Μ	Α	Η	Α	Ω	Γ	Ν	Δ	Κ	Λ
Ο	Α	Δ	Ξ	Δ	Ο	Ε	Σ	Ρ	Η	Η	Θ	Δ	Α	Ρ
Ν	Π	Μ	Ε	Θ	Λ	Δ	Ρ	Α	Ω	Σ	Ε	Π	Λ	Υ
Ο	Ε	Α	Α	Π	Ο	Ι	Ξ	Κ	Ν	Ο	Τ	Χ	Υ	Π
Μ	Κ	Ρ	Τ	Ρ	Γ	Κ	Γ	Α	Ν	Ψ	Β	Ζ	Ψ	Ρ
Χ	Φ	Ι	Α	Ρ	Η	Τ	Ω	Μ	Ψ	Ψ	Λ	Ζ	Η	Θ
Μ	Π	Κ	Μ	Μ	Σ	Υ	Σ	Ψ	Ξ	Η	Ο	Π	Η	Ω
Α	Ξ	Υ	Ζ	Υ	Η	Ο	Β	Η	Ψ	Ρ	Ψ	Β	Η	Μ

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ



ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

3 οριζόντια: ΦΙΛΤΡΟ Προηγμένος αποκλεισμός διαφημίσεων, κακόβουλου λογισμικού και μηνυμάτων συγκατάθεσης για cookie (6 γράμματα)

5 οριζόντια: ΔΡΟΜΟΛΟΓΗΣΗ Λειτουργία διπλού VPN που περνά την κίνηση μέσω δύο διαφορετικών κόμβων διακομιστή (11 γράμματα)

6 οριζόντια: ΔΙΑΚΟΠΤΗΣ Αυτόματη λειτουργία ασφαλείας που μπλοκάρει την κίνηση του δικτύου όταν πέσει το VPN (9 γράμματα)

7 οριζόντια: ΣΥΓΚΑΛΥΨΗ Τεχνολογία συσκότισης που κρύβει τις υπογραφές VPN ώστε να μοιάζουν με κανονική κίνηση HTTPS (9 γράμματα)

8 οριζόντια: ΠΑΡΑΚΑΜΨΗ Λειτουργία διαχωρισμού σήραγγας που επιτρέπει σε επιλεγμένες εφαρμογές να αγνοούν το VPN (9 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΕΝΑΛΛΑΓΗ Λειτουργία που αλλάζει τακτικά την εξωτερική σου διεύθυνση IP χωρίς να διακόπτει τις σήραγγες (8 γράμματα)

2 κάθετα: ΔΙΚΤΥΟ Ιδιόκτητη υποδομή ορισμένη από λογισμικό που συνδέει όλους τους διακομιστές σε ενιαίο πλέγμα (6 γράμματα)

4 κάθετα: ΜΟΝΟΜΝΗΜΗ Υλικό διακομιστή με πτητική μνήμη που σβήνει όλα τα δεδομένα σε κάθε επανεκκίνηση (9 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

Κλειδί βαθμολόγησης για τη δραστηριότητα αποκωδικοποίησης λέξεων λεξιλογίου και την πρόκληση Secret Cipher.

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΛΦΤΡΟΙ — **ΦΙΛΤΡΟ**
2. ΟΗΡΔΣΛΟΗΓΟΜ — **ΔΡΟΜΟΛΟΓΗΣΗ**
3. ΠΑΚΑΜΗΑΨΡ — **ΠΑΡΑΚΑΜΨΗ**
4. ΟΤΚΥΔΙ — **ΔΙΚΤΥΟ**
5. ΗΜΟΗΝΟΜΜΝ — **ΜΟΝΟΜΝΗΜΗ**
6. ΨΚΥΥΛΣΑΗΓ — **ΣΥΓΚΑΛΥΨΗ**
7. ΠΔΗΣΤΚΙΟΑ — **ΔΙΑΚΟΠΤΗΣ**
8. ΛΝΛΗΕΓΑΑ — **ΕΝΑΛΛΑΓΗ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΕΝΑΛΛΑΓΗ ΔΙΕΥΘΥΝΣΕΩΝ ΕΝΙΣΧΥΕΙ ΤΟ ΑΠΟΡΡΗΤΟ"

Λύσεις των μελετών περίπτωσης

A ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΠΑΡΑΚΑΜΨΗ ΦΙΛΤΡΩΝ CAMPUS ΚΑΙ ΧΩΡΟΥ ΕΡΓΑΣΙΑΣ

Λύση για τον εκπαιδευτικό

ΚΡΙΤΗΡΙΑ ΒΑΘΜΟΛΟΓΗΣΗΣ ΚΑΙ ΟΔΗΓΙΕΣ ΛΥΣΗΣ

- Ανάλυση σεναρίου: Ένας φοιτητής διαπιστώνει ότι το Wi-Fi της πανεπιστημιούπολής του αποκλείει όλες τις τυπικές θύρες OpenVPN και WireGuard.
- Ερώτηση εστίασης: Ποιο χαρακτηριστικό της Surfshark επιτρέπει στον φοιτητή να συνδεθεί χωρίς να εντοπιστεί από τους διαχειριστές του δικτύου;
- Προτεινόμενη στρατηγική και λύση: Ενεργοποίησε τη λειτουργία Camouflage Mode (OpenVPN), η οποία κρύβει τα μεταδεδομένα του VPN ώστε τα τείχη προστασίας να βλέπουν συνηθισμένη περιήγηση HTTPS.

B ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΔΗΜΟΣΙΟΓΡΑΦΙΚΗ ΕΡΕΥΝΑ ΥΨΗΛΟΥ ΚΙΝΔΥΝΟΥ

Λύση για τον εκπαιδευτικό

ΚΡΙΤΗΡΙΑ ΒΑΘΜΟΛΟΓΗΣΗΣ ΚΑΙ ΟΔΗΓΙΕΣ ΛΥΣΗΣ

- Ανάλυση σεναρίου: Ένας ερευνητής δημοσιογράφος χρειάζεται επιπλέον προστασία από την παρακολούθηση ενώ ερευνά ευαίσθητα εταιρικά αρχεία.
- Ερώτηση εστίασης: Πώς προσφέρει το Dynamic MultiHop ανώτερη ιδιωτικότητα σε σύγκριση με τη δρομολόγηση μέσω ενός μόνο διακομιστή;
- Προτεινόμενη στρατηγική και λύση: Το Dynamic MultiHop δρομολογεί την κίνηση μέσω διακομιστών εισόδου και εξόδου σε δύο χώρες, ώστε κανένας μεμονωμένος διακομιστής να μην μπορεί να εκθέσει τον χρήστη.