Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

Ασφάλεια ProtonVPN

Ανάλυση της αρχιτεκτονικής ασφαλείας του ProtonVPN, συμπεριλαμβανομένων των διακομιστών Secure Core, του φιλτραρίσματος DNS NetShield, της ελβετικής δικαιοδοσίας ιδιωτικότητας, των ελεγμένων εφαρμογών ανοιχτού κώδικα και του πρωτοκόλλου Stealth.

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ: ΑΣΦΑΛΕΙΑ PROTONVPN

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 του Proton VPN. Θα εξερευνήσεις διακομιστές διπλού άλματος Secure Core, αποκλεισμό DNS NetShield, ελβετικούς νόμους ιδιωτικότητας και συσκότιση Stealth.

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/protonvpn/asfalia/

Η πορεία μάθησής σου: ασφάλεια ProtonVPN

- Ανάλυσε την τεχνική αρχιτεκτονική και τους κανόνες διαμόρφωσης του ProtonVPN (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 ΓΙΑ ΤΟΝ ΟΔΗΓΟ ΑΣΦΑΛΕΙΑΣ PROTONVPN

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 στη δρομολόγηση διπλού άλματος Secure Core και στη διακυβέρνηση ιδιωτικότητας της Ελβετίας. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΠΛΟΥ ΒΗΜΑΤΟΣ SECURE CORE ΚΑΙ ΕΛΒΕΤΙΚΗ ΔΙΚΑΙΟΔΟΣΙΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Το Proton VPN προστατεύει την κίνηση των χρηστών με διακομιστές Secure Core ιδιοκτησίας της Proton στην Ελβετία, την Ισλανδία και τη Σουηδία, με ελεγμένες εφαρμογές ανοιχτού κώδικα και το πρωτόκολλο συσκότισης Stealth που έχει σχεδιαστεί για να παρακάμπτει τη βαθιά επιθεώρηση πακέτων.

(ΕΙΣΑΓΩΓΗ)

Το Proton VPN προστατεύει την κίνηση των χρηστών με διακομιστές Secure Core ιδιοκτησίας της Proton στην Ελβετία, την Ισλανδία και τη Σουηδία, με ελεγμένες εφαρμογές ανοιχτού κώδικα και το πρωτόκολλο συσκότισης Stealth που έχει σχεδιαστεί για να παρακάμπτει τη βαθιά επιθεώρηση πακέτων.

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **1. Τι είδους εγκαταστάσεις φιλοξενούν τους διακομιστές Secure Core του Proton;**
   - A) Εικονικές μηχανές δημόσιου cloud
   - B) Χώροι υψηλής ασφάλειας
   - C) Δημόσια κέντρα δεδομένων
   - D) Κοινόχρηστα rack

2. **2. Ποιο πρωτόκολλο βοηθά στην παράκαμψη της αυστηρής κρατικής λογοκρισίας;**
   - A) PPTP
   - B) Πρωτόκολλο Stealth
   - C) OpenVPN UDP
   - D) IKEv2

3. **3. Ποια είναι η λειτουργία του χαρακτηριστικού NetShield του Proton VPN;**
   - A) Speed Booster
   - B) Αποκλεισμός διαφημίσεων και κακόβουλου λογισμικού μέσω DNS
   - C) Αποθήκευση cloud
   - D) Προώθηση θυρών

4. **4. Βάσει των νόμων ιδιωτικότητας ποιας χώρας λειτουργεί η Proton AG;**
   - A) Ηνωμένες Πολιτείες
   - B) Ηνωμένο Βασίλειο
   - C) Ελβετία
   - D) Παναμάς

5. **5. Πώς επαληθεύονται από ειδικούς οι εφαρμογές πελάτη του Proton VPN;**
   - A) Μυστικός κωδικός
   - B) Έλεγχοι ανοιχτού κώδικα
   - C) Ιδιόκτητη άδεια χρήσης
   - D) Κυβερνητική αξιολόγηση

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Το Secure Core δρομολογεί την κίνηση μέσω χωρών φιλικών προς το απόρρητο πριν από την έξοδο.

Σωστό Λάθος

7 Ερώτηση 7

7. Η Ελβετία είναι μέλος της συμμαχίας κατασκοπείας 14 Eyes.

Σωστό Λάθος

8 Ερώτηση 8

8. Το NetShield αποκλείει διαφημίσεις και κακόβουλα ονόματα τομέα απευθείας στο επίπεδο DNS.

Σωστό Λάθος

9 Ερώτηση 9

9. Οι εφαρμογές του Proton VPN είναι 100% ανοιχτού κώδικα και ελέγχονται δημόσια.

Σωστό Λάθος

10 Ερώτηση 10

10. Το πρωτόκολλο Stealth χρησιμοποιεί τυπικές κεφαλίδες WireGuard χωρίς συσκότιση.

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. Η πολυβηματική δρομολόγηση μέσω διακομιστών ιδιοκτησίας Proton σε χώρες φιλικές προς το απόρρητο ονομάζεται αρχιτεκτονική _____ .

2. Για να παρακάμψουν την επιθεώρηση πακέτων (DPI) και τα τείχη προστασίας, οι χρήστες ενεργοποιούν τη λειτουργία _____ .

3. Τα κακόβουλα domains, οι ιχνηλάτες και τα σενάρια διαφημίσεων φιλτράρονται από το DNS του _____ .

4. Η Proton αναφέρει ότι υπό το ισχύον καθεστώς, δηλαδή το _____ , δεν υποχρεούται να κρατά αρχεία δραστηριότητας των χρηστών.

5. Αν η σήραγγα VPN αποσυνδεθεί απροσδόκητα, η κίνηση μπλοκάρεται από τον _____ ασφαλείας.

6. Ανεξάρτητοι ερευνητές ασφαλείας επαληθεύουν την ακεραιότητα του πελάτη επειδή οι εφαρμογές έχουν _____ κώδικα.

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΑΝΟΙΧΤΟ ΔΙΑΚΟΠΤΗΣ ΔΙΑΡΡΟΗ ΕΛΒΕΤΙΚΟ ΔΙΚΑΙΟ ΚΡΥΠΤΟΓΡΑΦΗΣΗ
NETSHIELD SECURE CORE STEALTH

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών VPN και δικτύου

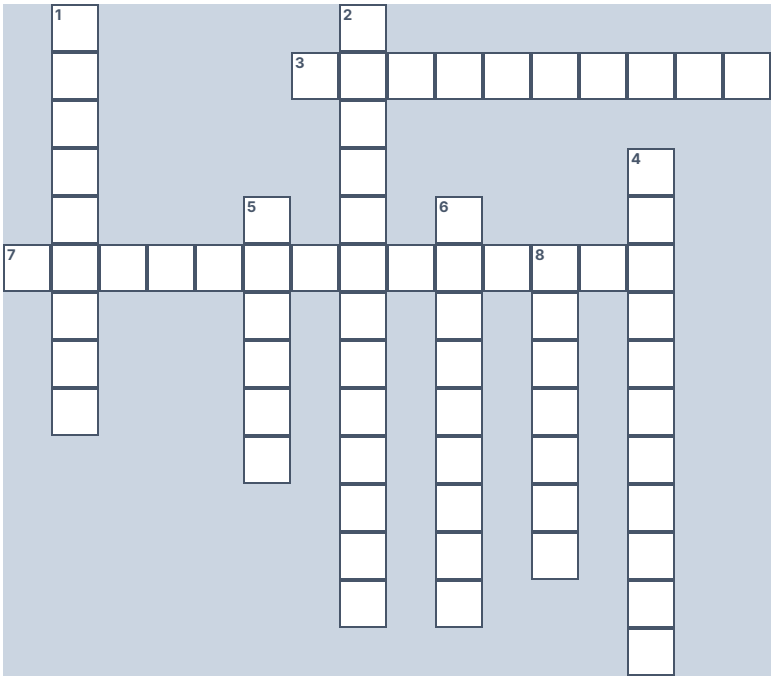
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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

☐	1. ΔΡΟΜΟΛΟΓΗΣΗ	A	Λογισμικό εφαρμογής πελάτη που είναι δημόσια προσβάσιμο και ελέγχεται ανεξάρτητα.
☐	2. ΣΥΓΚΑΛΥΨΗ	B	Πρότυπο συμμετρικού κρυπτογράφου που κρυπτογραφεί τα πακέτα δεδομένων του VPN.
☐	3. ΦΙΛΤΡΟ	C	Αυστηρά νομικά καθεστώτα απορρήτου στην Ελβετία, εκτός της δικαιοδοσίας των 14 Eyes.
☐	4. ΕΛΒΕΤΙΚΟ ΔΙΚΑΙΟ	D	Ένα πρωτόκολλο σηραγγοποίησης με συγκάλυψη που μεταμφιέζεται σε τυπική κίνηση ιστού HTTPS.
☐	5. ΔΙΑΚΟΠΤΗΣ	E	Ένα σύγχρονο ελαφρύ πρωτόκολλο που παρέχει ισχυρή κρυπτογραφία και γρήγορες ταχύτητες.
☐	6. ΑΝΟΙΧΤΟ	F	Ένα φίλτρο βασισμένο σε DNS που αποκλείει διαφημίσεις, εργαλεία παρακολούθησης τηλεμετρίας και κακόβουλο λογισμικό.
☐	7. ΠΡΩΤΟΚΟΛΛΟ	G	Σχεδιασμός πολλαπλών αναπηδήσεων που δρομολογεί την κίνηση μέσω διακομιστών πρώτης αναπήδησης ιδιοκτησίας του Proton.
☐	8. ΚΡΥΠΤΟΓΡΑΦΗΣΗ	H	Ένας μηχανισμός ασφαλείας που σταματά τη μετάδοση δικτύου όταν πέφτει η σύνδεση.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

3. Σύγχρονο ελαφρύ σύνολο κανόνων με ισχυρή κρυπτογραφία και υψηλές ταχύτητες (10)

7. Αυστηρή νομοθεσία απορρήτου στην Ελβετία, εκτός δικαιοδοσιών των 14 Eyes (14)

ΚΑΘΕΤΑ

1. Μέθοδος σήραγγας με συσκότιση που μοιάζει με κανονική κίνηση ιστού HTTPS (9)

2. Συμμετρική κρυπτογράφηση στρατιωτικού επιπέδου (AES-GCM) που ασφαλίζει όλα τα ενθυλακωμένα πακέτα δεδομένων VPN (13)

4. Σχεδίαση πολλαπλών βημάτων που περνά την κίνηση μέσω διακομιστών πρώτου βήματος ιδιοκτησίας Proton (11)

5. Σύστημα βάσει DNS που μπλοκάρει διαφημίσεις, ιχνηλάτες τηλεμετρίας και κακόβουλο λογισμικό (6)

6. Μηχανισμός ασφαλείας που σταματά τη μετάδοση δικτύου όταν πέσει η σύνδεση (9)

8. Λογισμικό εφαρμογών-πελατών που είναι δημόσια προσβάσιμο και ελέγχεται ανεξάρτητα (ανοιχτός κώδικας) (7)

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: Σύγχρονο ελαφρύ σύνολο κανόνων με ισχυρή κρυπτογραφία και υψηλές ταχύτητες (10 γράμματα):

7 οριζόντια: Αυστηρή νομοθεσία απορρήτου στην Ελβετία, εκτός δικαιοδοσιών των 14 Eyes (14 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Μέθοδος σήραγγας με συσκότιση που μοιάζει με κανονική κίνηση ιστού HTTPS (9 γράμματα):

2 κάθετα: Συμμετρική κρυπτογράφηση στρατιωτικού επιπέδου (AES-GCM) που ασφαλίζει όλα τα ενθυλακωμένα πακέτα δεδομένων VPN (13 γράμματα):

4 κάθετα: Σχεδίαση πολλαπλών βημάτων που περνά την κίνηση μέσω διακομιστών πρώτου βήματος ιδιοκτησίας Proton (11 γράμματα):

5 κάθετα: Σύστημα βάσει DNS που μπλοκάρει διαφημίσεις, ιχνηλάτες τηλεμετρίας και κακόβουλο λογισμικό (6 γράμματα):

6 κάθετα: Μηχανισμός ασφαλείας που σταματά τη μετάδοση δικτύου όταν πέσει η σύνδεση (9 γράμματα):

8 κάθετα: Λογισμικό εφαρμογών-πελατών που είναι δημόσια προσβάσιμο και ελέγχεται ανεξάρτητα (ανοιχτός κώδικας) (7 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.

Η Ρ Γ Α Λ Ο Γ Ω Μ Κ Φ Ρ Υ Α Ρ

Σ Χ Ο Λ Λ Ο Κ Ο Τ Ω Ρ Π Κ Μ Μ

Η Η Θ Ν Α Ν Ο Ι Χ Τ Ο Θ Π Ζ Λ

Φ Σ Λ Ρ Χ Θ Β Τ Ζ Ψ Ξ Ψ Χ Σ Η

Α Τ Φ Χ Α Ο Υ Ν Ν Ω Ξ Θ Ο Σ Θ

Ρ Ο Ι Υ Τ Ξ Υ Τ Κ Α Ε Ξ Μ Λ Α

Γ Ν Λ Υ Ζ Η Ο Π Χ Ψ Ι Κ Υ Ι Ω

Ο Φ Τ Ψ Ο Σ Η Τ Π Ο Κ Α Ι Δ Κ

Τ Θ Ρ Ω Ι Ι Ν Α Ε Θ Α Σ Α Ι Ε

Π Φ Ο Η Ψ Υ Λ Α Κ Γ Υ Σ Ε Κ Ω

Υ Ε Λ Β Ε Τ Ι Κ Ο Δ Ι Κ Α Ι Ο

Ρ Κ Ε Κ Π Ν Ι Α Ζ Ξ Κ Ν Γ Ν Γ

Κ Δ Δ Ρ Ο Μ Ο Λ Ο Γ Η Σ Η Η Θ

Β Α Ξ Ρ Λ Ο Φ Τ Θ Ψ Ζ Ω Ρ Η Χ

Φ Θ Ε Π Τ Ν Τ Κ Ρ Δ Τ Σ Λ Ο Λ

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΔΡΟΜΟΛΟΓΗΣΗ ΣΥΓΚΑΛΥΨΗ ΦΙΛΤΡΟ ΕΛΒΕΤΙΚΟΔΙΚΑΙΟ ΔΙΑΚΟΠΤΗΣ
ΑΝΟΙΧΤΟ ΠΡΩΤΟΚΟΛΛΟ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

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. ΔΡΟΜΟΛΟΓΗΣΗ
B. ΣΥΓΚΑΛΥΨΗ
C. ΦΙΛΤΡΟ
D. ΕΛΒΕΤΙΚΟΔΙΚΑΙΟ
E. ΔΙΑΚΟΠΤΗΣ
F. ΑΝΟΙΧΤΟ
G. ΠΡΩΤΟΚΟΛΛΟ
H. ΚΡΥΠΤΟΓΡΑΦΗΣΗ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ	
	1. Μέθοδος σήραγγας με συσκότιση που μοιάζει με κανονική κίνηση ιστού HTTPS.
	2. Σύγχρονο ελαφρύ σύνολο κανόνων με ισχυρή κρυπτογραφία και υψηλές ταχύτητες.
	3. Αυστηρή νομοθεσία απορρήτου στην Ελβετία, εκτός δικαιοδοσιών των 14 Eyes.
	4. Σχεδίαση πολλαπλών βημάτων που περνά την κίνηση μέσω διακομιστών πρώτου βήματος ιδιοκτησίας Proton.
	5. Συμμετρική κρυπτογράφηση στρατιωτικού επιπέδου (AES-GCM) που ασφαλίζει όλα τα ενθυλακωμένα πακέτα δεδομένων VPN.
	6. Μηχανισμός ασφαλείας που σταματά τη μετάδοση δικτύου όταν πέσει η σύνδεση.
	7. Σύστημα βάσει DNS που μπλοκάρει διαφημίσεις, ιχνηλάτες τηλεμετρίας και κακόβουλο λογισμικό.
	8. Λογισμικό εφαρμογών-πελατών που είναι δημόσια προσβάσιμο και ελέγχεται ανεξάρτητα (ανοιχτός κώδικας).

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. ΟΟΣΡΛΓΔΗΟΗΜ
2. ΟΦΛΡΤΙ
3. ΔΠΟΙΤΣΚΗΑ
4. ΚΛΟΟΤΛΟΠΡΩ
5. ΥΑΥΗΛΚΣΨΓ
6. ΙΚΚΤΒΑΟΙΙΕΛΔΟΕ
7. ΑΤΧΟΝΙΟ
8. ΑΥΤΟΗΡΗΚΓΡΣΦΠ

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	Πράγματα που κάνεις online κάθε μέρα			
2	Χώρες γνωστές για τους ισχυρούς νόμους απορρήτου			
3	Λειτουργίες ασφάλειας στο Proton VPN			
4	Τύποι διαρροών VPN			
5	Καταστάσεις όπου βοηθά ένα kill switch			
6	Πράγματα που μπορεί να ελέγξει ένας έλεγχος (audit)			
7	Ρυθμίσεις που ενεργοποιείς για επιπλέον ασφάλεια			
8	Πράγματα που προστατεύει η κρυπτογράφηση			
9	Λέξεις που περιγράφουν μια καλή εφαρμογή VPN			
10	Λόγοι για τους οποίους θα επέλεγες το Proton VPN			
11	Κουμπιά ή μενού σε μια εφαρμογή VPN			
12	Υπηρεσίες streaming που παρακολουθείς			
13	Απειλές στο δημόσιο Wi-Fi			
14	Τρόποι να φτιάξεις έναν ισχυρό κωδικό πρόσβασης			
15	Χώρες όπου θα ήθελες διακομιστές Proton VPN			

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 ΠΕΡΙΟΡΙΣΤΙΚΩΝ ΤΕΙΧΩΝ ΠΡΟΣΤΑΣΙΑΣ



Σενάριο: Ένας χρήστης ταξιδεύει σε χώρα όπου η τυπική κίνηση VPN, όπως OpenVPN και WireGuard, μπλοκάρεται από DPI.

Ερώτηση συζήτησης: Ποια διαμόρφωση πρωτοκόλλου του Proton VPN επιτρέπει στον χρήστη να παρακάμψει τον έλεγχο σε επίπεδο κράτους;

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΠΡΟΗΓΜΕΝΗ ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΑΝΤΙΠΑΛΟΥΣ



Σενάριο: Ένας οικονομικός ελεγκτής υποπτεύεται ότι ο κόμβος εξόδου του τοπικού παρόχου internet του μπορεί να έχει παραβιαστεί από προηγμένες επίμονες απειλές.

Ερώτηση συζήτησης: Πώς προστατεύει το Secure Core την ταυτότητα του ελεγκτή σε περίπτωση παραβίασης κόμβου εξόδου;

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

15	22	20	17	24	12	5	13	15	9

4	9	1	10	15	12	9	18	19	5	18

16	17	15	18	19	1	19	5	20	15	20	13

4	5	4	15	12	5	13	1

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 Proton VPN Secure Core;

Το Secure Core δρομολογεί την κίνηση μέσω πολλών διακομιστών σε χώρες φιλικές προς το απόρρητο πριν από την έξοδο.

Q2: Τι είναι το πρωτόκολλο Stealth;

Το Stealth είναι ένα πρωτόκολλο απόκρυψης που κρύβει τις συνδέσεις VPN ως κανονική κίνηση TLS/HTTPS.

Q3: Πώς προστατεύει τους χρήστες το NetShield;

Το NetShield είναι ένα εργαλείο βασισμένο σε DNS που αποκλείει αυτόματα διαφημίσεις, ιχνηλάτες και ονόματα τομέα κακόβουλου λογισμικού.

Q4: Προστατεύεται νομικά το Proton VPN στην Ελβετία;

Ναι, η Ελβετία έχει αυστηρούς νόμους ιδιωτικότητας και βρίσκεται εκτός της δικαιοδοσίας των ΗΠΑ και της ΕΕ/14 Eyes. [4]

Q5: Είναι ανοιχτού κώδικα οι εφαρμογές του Proton VPN;

Ναι. Οι εφαρμογές του Proton VPN είναι ανοιχτού κώδικα και έχουν υποβληθεί σε δημοσιευμένους ελέγχους ασφαλείας.

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: Ποιοι κρυπτογραφικοί αλγόριθμοι χρησιμοποιούνται;

Το Proton VPN χρησιμοποιεί AES-256-GCM ή ChaCha20-Poly1305 με χειραψίες HMAC-SHA384 και RSA-4096.

Q7: Διαθέτει το Proton VPN Kill Switch;

Ναι, το Proton VPN περιλαμβάνει τυπικό και Μόνιμο Kill Switch για την αποφυγή μη κρυπτογραφημένων διαρροών.

Q8: Μπορεί το Proton VPN να διαρρεύσει ερωτήματα DNS;

Όχι, όλα τα ερωτήματα DNS δρομολογούνται μέσω κρυπτογραφημένων ιδιωτικών διακομιστών DNS που ανήκουν στην Proton.

Q9: Διατηρεί αρχεία καταγραφής συνδέσεων το Proton VPN;

Όχι, το Proton VPN τηρεί αυστηρή πολιτική μη καταγραφής, που επιβεβαιώνεται από ετήσιους ελέγχους της Securitum. [3]

Q10: Είναι ευάλωτο το Proton VPN σε διαρροές WebRTC;

Όχι, οι πελάτες της Proton περιλαμβάνουν ενσωματωμένους κανόνες τείχους προστασίας και πολιτικές δρομολόγησης που αποκλείουν τις διαρροές WebRTC.

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: Πού βρίσκονται φυσικά τα κέντρα δεδομένων Secure Core;

Βρίσκονται στην Ελβετία, σε μια πρώην στρατιωτική βάση στην Ισλανδία και σε ένα υπόγειο χώρο στη Σουηδία. [1]

Q2: Πώς λειτουργεί το Perfect Forward Secrecy στο Proton VPN;

Δημιουργείται ένα μοναδικό εφήμερο κλειδί κρυπτογράφησης για κάθε συνεδρία, αποτρέποντας την αναδρομική αποκρυπτογράφηση.

Q3: Τι είναι το Permanent Kill Switch στα Windows/Linux;

Ο μόνιμος διακόπτης kill switch αποκλείει όλη την κίνηση δικτύου ακόμη και αν η εφαρμογή VPN κλείσει εντελώς ή καταρρεύσει.

Q4: Υποστηρίζει το Proton VPN δρομολόγηση IPv6 και άμυνα έναντι διαρροών;

Το Proton VPN δρομολογεί πλήρως την κίνηση IPv6 μέσω των τούνελ ή την απενεργοποιεί με ασφάλεια για να αποτρέψει διαρροές.

Q5: Πώς χειρίζεται το φιλτράρισμα DNS του NetShield την επιθεώρηση HTTPS;

Το NetShield λειτουργεί αποκλειστικά στο επίπεδο επίλυσης DNS, χωρίς να απαιτεί παρεμβατική αποκρυπτογράφηση TLS.

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: Ποιος πραγματοποίησε τους ελέγχους κώδικα τρίτων του Proton VPN;

Η SEC Consult έλεγξε τις εφαρμογές, ενώ η Securitum ελέγχει τις εφαρμογές και την πολιτική μη τήρησης αρχείων καταγραφής.

Q7: Πώς συγκρίνεται το πρωτόκολλο Stealth με το OpenVPN XOR ή το Shadowsocks;

Το Stealth διοχετεύει το WireGuard μέσω αποκρυμμένου TLS και υπερέχει σε απόδοση από την παλαιότερη απόκρυψη που βασίζεται στο OpenVPN. [5]

Q8: Μπορούν οι ελβετικές αρχές να υποχρεώσουν το Proton VPN να καταγράφει κίνηση;

Η Proton δηλώνει ότι βάσει του ελβετικού νόμου δεν υποχρεούται να διατηρεί αρχεία καταγραφής ή δεδομένα δραστηριότητας των χρηστών.

Q9: Πώς προστατεύονται οι διακομιστές του Proton VPN από κατάσχεση;

Όλοι οι διακομιστές του Proton VPN είναι μηχανήματα bare-metal προστατευμένα με κρυπτογράφηση ολόκληρου του δίσκου. [2]

Q10: Υποστηρίζει το Proton VPN προσαρμοσμένες διαμορφώσεις διακομιστών DNS;

Ναι, οι συνδρομητές επί πληρωμή μπορούν να ορίσουν προσαρμοσμένους διακομιστές DNS ανάντη απευθείας στις προτιμήσεις της εφαρμογής.

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 Proton κατέχει και εγκαθιστά η ίδια τους διακομιστές Secure Core, σε χώρους υψηλής ασφάλειας στην Ελβετία, την Ισλανδία και τη Σουηδία. [1]

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

2. Οι εφαρμογές πελάτη του Proton VPN είναι ανοιχτού κώδικα και υποβάλλονται σε επαναλαμβανόμενους ελέγχους κώδικα από τρίτους.

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

3. Το πρωτόκολλο απόκρυψης Stealth παρακάμπτει την ανάλυση βάθους πακέτων (DPI) προσομοιώνοντας τυπική κίνηση TLS.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

4. Η Ελβετία βρίσκεται εκτός των διεθνών συμμαχιών ανταλλαγής πληροφοριών 5-Eyes, 9-Eyes και 14-Eyes. [4]

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

5. Το NetShield λειτουργεί σε επίπεδο επίλυσης DNS, αποτρέποντας διαφημίσεις και κακόβουλο λογισμικό πριν από τη λήψη του φορτίου.

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

6. Το Perfect Forward Secrecy διασφαλίζει ότι τα παραβιασμένα κλειδιά δεν μπορούν να αποκρυπτογραφήσουν συνεδρίες κίνησης που έχουν καταγραφεί προηγουμένως. [7]

7. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

7. Το Proton VPN χρησιμοποιεί κρυπτογράφηση ολόκληρου του δίσκου σε διακομιστές bare-metal για την προστασία των ρυθμίσεων των διακομιστών. [2]

8. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

8. Ο Μόνιμος Kill Switch αποτρέπει διαρροές μη κρυπτογραφημένων δεδομένων ακόμη και κατά τις επανεκκινήσεις του λειτουργικού συστήματος.

9. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

9. Η Securitum έχει ελέγξει και επιβεβαιώσει την πολιτική μη τήρησης αρχείων καταγραφής του Proton VPN σε πέντε συνεχόμενους ετήσιους ελέγχους. [3]

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

10. Το Proton VPN αναπτύχθηκε από επιστήμονες που γνωρίστηκαν στο CERN (Ευρωπαϊκός Οργανισμός Πυρηνικών Ερευνών). [4]

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] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[2] Proton VPN. (n.d.). Proton VPN features.
https://protonvpn.com/features

[3] Proton VPN. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.
https://protonvpn.com/blog/no-logs-audit

[4] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.
https://protonvpn.com/features/swiss-based

[5] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.
https://protonvpn.com/blog/stealth-vpn-protocol

[6] GitHub. (n.d.). ProtonVPN · GitHub.
https://github.com/ProtonVPN

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

[8] IETF. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[9] NIST. (2007). SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.
https://csrc.nist.gov/pubs/sp/800/38/d/final

[10] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.
https://www.rfc-editor.org/rfc/rfc7359

[11] IETF. (2021). RFC 9076: DNS Privacy Considerations.
https://www.rfc-editor.org/rfc/rfc9076

[12] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).
https://www.edoeb.admin.ch/en

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 **Ερώτηση 1** — **Σωστή απάντηση: B**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι διακομιστές Secure Core βρίσκονται σε χώρους υψηλής ασφάλειας, μεταξύ των οποίων μια πρώην στρατιωτική βάση στην Ισλανδία και ένα υπόγειο κέντρο δεδομένων στη Σουηδία.

2 **Πρωτόκολλο απόκρυψης Stealth** — ΑΜΥΝΑ ΑΠΕΝΑΝΤΙ ΣΤΗ ΛΟΓΟΚΡΙΣΙΑ — **Σωστή απάντηση: B**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το πρωτόκολλο Stealth της Proton μεταμφιέζει τις συνδέσεις WireGuard ως τυπική κίνηση TLS/HTTPS για να παρακάμπτει τα τείχη προστασίας Βαθιάς Επιθεώρησης Πακέτων (DPI). Παραπομπή: Proton Stealth Protocol Whitepaper.

3 **Αποκλεισμός διαφημίσεων DNS NetShield** — ΦΙΛΤΡΑΡΙΣΜΑ DNS — **Σωστή απάντηση: B**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το NetShield χρησιμοποιεί φιλτράρισμα σε επίπεδο DNS για να αποκλείει ονόματα τομέα κακόβουλου λογισμικού, λογισμικό κατασκοπείας, παρεμβατικές διαφημίσεις και ιχνηλάτες τηλεμετρίας πριν φορτώσουν οι ιστοσελίδες. Παραπομπή: NetShield Security Specs.

4 **Ελβετική νομική δικαιοδοσία** — ΔΙΚΑΙΟΔΟΣΙΑ — **Σωστή απάντηση: C**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η Proton AG έχει έδρα στη Γενεύη της Ελβετίας, επωφελούμενη από ισχυρούς ελβετικούς νόμους περί ιδιωτικότητας εκτός των συμμαχιών παρακολούθησης 14-Eyes των ΗΠΑ και της ΕΕ. Παραπομπή: Swiss Federal Data Protection Act. [4]

5 **Ερώτηση 5** — **Σωστή απάντηση: B**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Όλες οι εφαρμογές του Proton VPN είναι ανοιχτού κώδικα· η SEC Consult και αργότερα η Securitum τις έχουν ελέγξει.

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 Secure Core πολλαπλών δικαιοδοσιών

ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΡΟΜΟΛΟΓΗΣΗΣ

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το Secure Core δρομολογεί την κίνηση μέσω δικαιοδοσιών με ενισχυμένο απόρρητο πριν βγει στη χώρα προορισμού, βοηθώντας στην προστασία από έναν παραβιασμένο διακομιστή εξόδου.

7 Ελβετική συμμαχία επιτήρησης

ΣΥΜΜΑΧΙΕΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η Ελβετία δεν είναι μέλος των συμφωνιών ανταλλαγής πληροφοριών 5-Eyes, 9-Eyes ή 14-Eyes, διατηρώντας ανεξάρτητη νομική κυριαρχία. Παραπομπή: International Surveillance Treaties.

8 Ερώτηση 8

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το NetShield χρησιμοποιεί τους διακομιστές DNS του Proton για να ελέγχει τα domain σε λίστες γνωστών domain διαφημίσεων, ιχνηλατών και κακόβουλου λογισμικού.

9 Έλεγχος πελάτη ανοιχτού κώδικα

ΔΙΑΦΑΝΕΙΑ ΑΣΦΑΛΕΙΑΣ

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η Proton έχει κάνει τις εφαρμογές της για υπολογιστές και κινητά ανοιχτού κώδικα και δημοσιεύει εκθέσεις ελέγχου από τρίτους. Παραπομπή: SEC Consult Security Report.

10 Ερώτηση 10

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: το Stealth περικλείει το WireGuard σε αποκρυμμένο TLS πάνω από TCP, ώστε η κίνηση να μοιάζει με συνηθισμένο HTTPS.

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

G 1. ΔΡΟΜΟΛΟΓΗΣΗ	D 2. ΣΥΓΚΑΛΥΨΗ	F 3. ΦΙΛΤΡΟ	C 4. ΕΛΒΕΤΙΚΟ ΔΙΚΑΙΟ
H 5. ΔΙΑΚΟΠΤΗΣ	A 6. ΑΝΟΙΧΤΟ	E 7. ΠΡΩΤΟΚΟΛΛΟ	B 8. ΚΡΥΠΤΟΓΡΑΦΗΣΗ

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 SECURE CORE	2 STEALTH	3 NETSHIELD	4 ΕΛΒΕΤΙΚΟ ΔΙΚΑΙΟ
5 ΔΙΑΚΟΠΤΗΣ	6 ΑΝΟΙΧΤΟ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 B – ΣΥΓΚΑΛΥΨΗ	2 G – ΠΡΩΤΟΚΟΛΛΟ	3 D – ΕΛΒΕΤΙΚΟΔΙΚΑΙΟ	4 A – ΔΡΟΜΟΛΟΓΗΣΗ
5 H – ΚΡΥΠΤΟΓΡΑΦΗΣΗ	6 E – ΔΙΑΚΟΠΤΗΣ	7 C – ΦΙΛΤΡΟ	8 F – ΑΝΟΙΧΤΟ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους ΔΡΟΜΟΛΟΓΗΣΗ, ΣΥΓΚΑΛΥΨΗ και ΦΙΛΤΡΟ 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

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

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ

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

ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

3 οριζόντια: ΠΡΩΤΟΚΟΛΛΟ Σύγχρονο ελαφρύ σύνολο κανόνων με ισχυρή κρυπτογραφία και υψηλές ταχύτητες (10 γράμματα)

7 οριζόντια: ΕΛΒΕΤΙΚΟΔΙΚΑΙΟ Αυστηρή νομοθεσία απορρήτου στην Ελβετία, εκτός δικαιοδοσιών των 14 Eyes (14 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΣΥΓΚΑΛΥΨΗ Μέθοδος σήραγγας με συσκότιση που μοιάζει με κανονική κίνηση ιστού HTTPS (9 γράμματα)

2 κάθετα: ΚΡΥΠΤΟΓΡΑΦΗΣΗ Συμμετρική κρυπτογράφηση στρατιωτικού επιπέδου (AES-GCM) που ασφαλίζει όλα τα ενθυλακωμένα πακέτα δεδομένων VPN (13 γράμματα)

4 κάθετα: ΔΡΟΜΟΛΟΓΗΣΗ Σχεδίαση πολλαπλών βημάτων που περνά την κίνηση μέσω διακομιστών πρώτου βήματος ιδιοκτησίας Proton (11 γράμματα)

5 κάθετα: ΦΙΛΤΡΟ Σύστημα βάσει DNS που μπλοκάρει διαφημίσεις, ιχνηλάτες τηλεμετρίας και κακόβουλο λογισμικό (6 γράμματα)

6 κάθετα: ΔΙΑΚΟΠΤΗΣ Μηχανισμός ασφαλείας που σταματά τη μετάδοση δικτύου όταν πέσει η σύνδεση (9 γράμματα)

8 κάθετα: ΑΝΟΙΧΤΟ Λογισμικό εφαρμογών-πελατών που είναι δημόσια προσβάσιμο και ελέγχεται ανεξάρτητα (ανοιχτός κώδικας) (7 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

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

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΟΟΣΡΛΓΔΗΟΗΜ — **ΔΡΟΜΟΛΟΓΗΣΗ**
2. ΟΦΛΡΤΙ — **ΦΙΛΤΡΟ**
3. ΔΠΟΙΤΣΚΗΑ — **ΔΙΑΚΟΠΤΗΣ**
4. ΚΛΟΟΤΛΟΠΡΩ — **ΠΡΩΤΟΚΟΛΛΟ**
5. ΥΑΥΗΛΚΣΨΓ — **ΣΥΓΚΑΛΥΨΗ**
6. ΙΚΚΤΒΑΟΙΙΕΛΔΟΕ — **ΕΛΒΕΤΙΚΟΔΙΚΑΙΟ**
7. ΑΤΧΟΝΙΟ — **ΑΝΟΙΧΤΟ**
8. ΑΥΤΟΗΡΗΚΓΡΣΦΠ — **ΚΡΥΠΤΟΓΡΑΦΗΣΗ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΟΧΥΡΩΜΕΝΟΙ ΔΙΑΚΟΜΙΣΤΕΣ ΠΡΟΣΤΑΤΕΥΟΥΝ ΔΕΔΟΜΕΝΑ"

Λύσεις των μελετών περίπτωσης

A ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΠΑΡΑΚΑΜΨΗ ΠΕΡΙΟΡΙΣΤΙΚΩΝ ΤΕΙΧΩΝ ΠΡΟΣΤΑΣΙΑΣ

Λύση για τον εκπαιδευτικό

ΚΡΙΤΗΡΙΑ ΒΑΘΜΟΛΟΓΗΣΗΣ ΚΑΙ ΟΔΗΓΙΕΣ ΛΥΣΗΣ

- Ανάλυση σεναρίου: Ένας χρήστης ταξιδεύει σε χώρα όπου η τυπική κίνηση VPN, όπως OpenVPN και WireGuard, αποκλείεται από DPI.
- Ερώτηση εστίασης: Ποια ρύθμιση πρωτοκόλλου του Proton VPN επιτρέπει στον χρήστη να παρακάμψει τον έλεγχο σε επίπεδο κράτους;
- Προτεινόμενη στρατηγική και λύση: Ο χρήστης πρέπει να ενεργοποιήσει το πρωτόκολλο Stealth, που συγκαλύπτει τις κεφαλίδες των πακέτων VPN ως κανονική κίνηση ιστού TLS/HTTPS, περνώντας απαρατήρητο από τα φίλτρα DPI.

B ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΠΡΟΗΓΜΕΝΗ ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΑΝΤΙΠΑΛΟΥΣ

Λύση για τον εκπαιδευτικό

ΚΡΙΤΗΡΙΑ ΒΑΘΜΟΛΟΓΗΣΗΣ ΚΑΙ ΟΔΗΓΙΕΣ ΛΥΣΗΣ

- Ανάλυση σεναρίου: Ένας οικονομικός ελεγκτής υποψιάζεται ότι ο κόμβος εξόδου του τοπικού παρόχου διαδικτύου του μπορεί να έχει παραβιαστεί από προηγμένες επίμονες απειλές.
- Ερώτηση εστίασης: Πώς προστατεύει το Secure Core την ταυτότητα του ελεγκτή σε περίπτωση παραβίασης του κόμβου εξόδου;
- Προτεινόμενη στρατηγική και λύση: Το Secure Core δρομολογεί πρώτα την κίνηση μέσω διακομιστών ιδιοκτησίας της Proton στην Ελβετία, την Ισλανδία ή τη Σουηδία, ώστε ένας παραβιασμένος διακομιστής εξόδου να μην μπορεί να εντοπίσει την IP του χρήστη.