Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

Οδηγός για το ασφαλέστερο VPN

Τεχνική ανάλυση του σχεδιασμού VPN υψηλής ασφάλειας, διακομιστές με πτητική μνήμη μόνο RAM, ασφάλεια πρόσβασης Zero Trust, άμυνες ιδιωτικού κρυπτογραφημένου DNS κατά των διαρροών και ελεγμένες ρυθμίσεις WireGuard.

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ ΟΔΗΓΟΥ ΓΙΑ ΤΟ ΑΣΦΑΛΕΣΤΕΡΟ VPN

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 στα τεχνικά πρότυπα των πολύ ασφαλών VPN. Θα εξερευνήσεις υλικό διακομιστών μόνο RAM, ασφάλεια πρόσβασης Zero Trust, ιδιωτικούς κρυπτογραφημένους resolver DNS και ελεγμένες ρυθμίσεις WireGuard.

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/asfalestero-vpn/

Η πορεία μάθησής σου: το πιο ασφαλές VPN

- Ανάλυσε την τεχνική αρχιτεκτονική και τα πρότυπα κρυπτογράφησης: Most Secure VPN).
- Ρύθμισε τις παραμέτρους του πελάτη ώστε να αποτρέπονται οι διαρροές κίνησης IP, DNS και WebRTC.
- Σύγκρινε τα ιδιόκτητα πρωτόκολλα σηράγγωσης με τις τυπικές υλοποιήσεις.

ΟΔΗΓΙΕΣ ΟΔΗΓΟΥ ΓΙΑ ΤΟ ΑΣΦΑΛΕΣΤΕΡΟ VPN

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 στο υλικό διακομιστών μόνο RAM και στα συστήματα Zero Trust. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΥΠΟΔΟΜΕΣ ΜΟΝΟ ΜΕ RAM ΚΑΙ ΔΙΚΤΥΑ ΜΗΔΕΝΙΚΗΣ ΕΜΠΙΣΤΟΣΥΝΗΣ (ΕΙΣΑΓΩΓΗ)

Ένα πραγματικά ασφαλές VPN βασίζεται σε πλαίσιο μηδενικής εμπιστοσύνης (zero trust), διακομιστές μόνο RAM ώστε η κατάσχεση δίσκων να μην εκθέτει αρχεία καταγραφής, ιδιωτικούς κρυπτογραφημένους επιλύτες DNS και ελεγμένα πρωτόκολλα όπως το WireGuard. Αυτοί οι συνδυασμένοι έλεγχοι προστατεύουν πολύτιμα ψηφιακά περιουσιακά στοιχεία από απειλές υποκλοπής.

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **Ποια αρχιτεκτονική είναι θεμελιώδης για τη διασφάλιση της υψηλότερης ασφάλειας στους σύγχρονους διακομιστές VPN;**
   - A) Υποδομή διακομιστών μόνο RAM
   - B) Αποθήκευση σε δίσκο
   - C) Δυναμική δρομολόγηση DNS
   - D) Ενεργοποίηση προώθησης θυρών

2. **Ποιο πρωτόκολλο συνιστάται ευρέως για τις πιο ασφαλείς και σύγχρονες διαμορφώσεις VPN;**
   - A) WireGuard
   - B) PPTP
   - C) L2TP/IPSec
   - D) SSTP

3. **Ποιο πλαίσιο ασφάλειας απαιτεί συνεχή επαλήθευση κάθε σύνδεσης χωρίς εξαίρεση;**
   - A) Αρχιτεκτονική Zero Trust
   - B) Τείχη προστασίας περιμέτρου
   - C) Δυναμική δρομολόγηση
   - D) Κοινά μυστικά κλειδιά

4. **Ποιος είναι ο κύριος ρόλος της προστασίας από διαρροές DNS ενός πελάτη VPN;**
   - A) Δρομολόγηση όλων των αιτημάτων DNS μέσω ιδιωτικών κρυπτογραφημένων επιλυτών
   - B) Συσκότιση πακέτων IP
   - C) Τοπική προσωρινή αποθήκευση ερωτημάτων DNS
   - D) Απενεργοποίηση διακομιστών ονομάτων

5. **Πώς αυξάνει η δρομολόγηση Multi-Hop τη συνολική ασφάλεια μιας σήραγγας VPN;**
   - A) Δρομολογεί τα δεδομένα μέσω δύο ξεχωριστών διακομιστών σε σειρά
   - B) Αυξάνει την ταχύτητα συμπίεσης
   - C) Κρυπτογραφεί δεδομένα με κρυπτογραφικούς αλγορίθμους χαμηλής ασφάλειας
   - D) Παρακάμπτει τα τείχη προστασίας

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Οι διακομιστές μόνο με RAM αποθηκεύουν τα αρχεία καταγραφής σε προσωρινή μνήμη, η οποία διαγράφεται κατά την επανεκκίνηση.

○ Σωστό ○ Λάθος

7 Ερώτηση 7

7. Το WireGuard χρησιμοποιεί σύγχρονους κρυπτογραφικούς αλγορίθμους που είναι λιγότερο ευάλωτοι σε σημεία συμφόρησης ταχύτητας.

○ Σωστό ○ Λάθος

8 Ερώτηση 8

8. Ένας kill switch VPN λειτουργεί αποκλείοντας όλη την κίνηση δικτύου αν πέσει η σήραγγα.

○ Σωστό ○ Λάθος

9 Ερώτηση 9

9. Οι ανεξάρτητοι έλεγχοι από τρίτους είναι άσχετοι με την επαλήθευση των δεσμεύσεων ασφαλείας.

○ Σωστό ○ Λάθος

10 Ερώτηση 10

10. Τα μοντέλα Zero Trust θεωρούν όλες τις εσωτερικές συνδέσεις δικτύου ασφαλείς από προεπιλογή.

○ 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 διαχειριστές επιβάλλουν την ασφάλεια εφαρμόζοντας ένα αυστηρό πλαίσιο _____ .

2. Η δρομολόγηση πακέτων μέσω πολλών σημείων εισόδου απαιτεί μια ασφαλή διαμόρφωση _____ .

3. Για να αποτραπούν διαρροές δεδομένων από κλεμμένους δίσκους, χρησιμοποιούμε σχεδιασμό διακομιστών τύπου _____ .

4. Η υφαρπαγή από τον πάροχο διαδικτύου αντιμετωπίζεται ρυθμίζοντας την εγγενή _____ **DNS.**

5. Για να μπλοκάρεται η κίνηση κατά τις αποτυχίες σύνδεσης, ενεργοποίησε τον μηχανισμό: _____ .

6. Για να ελαχιστοποιήσεις τα αρχεία καταγραφής της βάσης δεδομένων, επίλεξε έναν πλήρως _____ **πάροχο.**

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΔΙΑΚΟΠΤΗΣ ΕΛΕΓΜΕΝΟ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΜΟΝΟ ΜΝΗΜΗ ΠΡΟΣΤΑΣΙΑ
ΤΑΥΤΟΠΟΙΗΣΗ MULTI-HOP ZERO TRUST

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών VPN και δικτύου

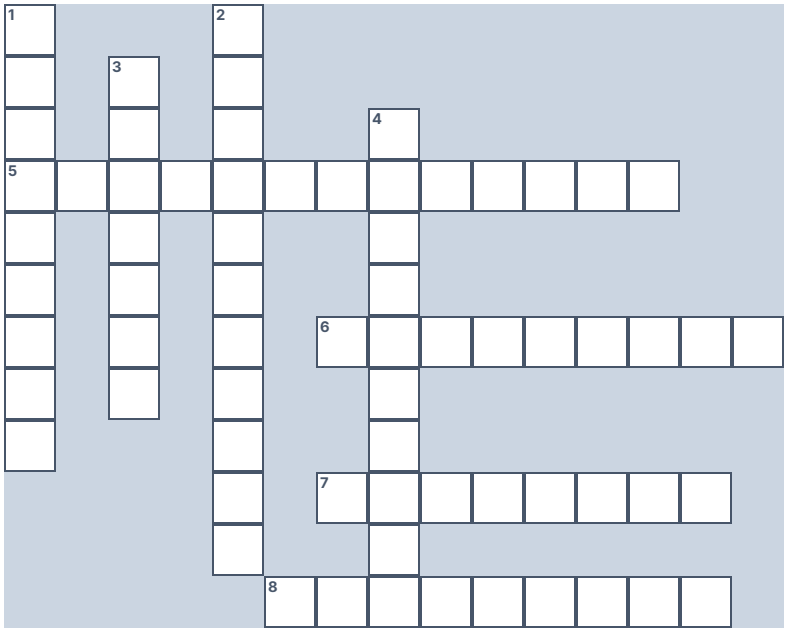
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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

☐	1. Zero Trust	A	Ανεξάρτητα ελεγμένη διάταξη που επιβεβαιώνει ότι δεν αποθηκεύονται καταγραφές.
☐	2. Multi-Hop	B	Κρυπτογραφικό ανακάτεμα των δεδομένων του ωφέλιμου φορτίου για ασφαλή μετάδοση.
☐	3. Διακομιστής μόνο με RAM	C	Πλαίσιο ασφαλείας που απαιτεί συνεχή ταυτοποίηση όλων των χρηστών.
☐	4. Προστασία DNS	D	Σύνολο τεχνικών κανόνων που καθορίζουν πώς πακετάρονται και αποστέλλονται τα δεδομένα.
☐	5. Kill switch	E	Διαδοχική δρομολόγηση VPN που αλυσιδώνει δύο κόμβους διακομιστών.
☐	6. Σύστημα με έλεγχο	F	Αρχιτεκτονική διακομιστή που χρησιμοποιεί πτητική μνήμη για την αποθήκευση φορτίων δεδομένων.
☐	7. Κρυπτογράφηση	G	Επιβολή ιδιωτικών ερωτημάτων DNS για την προστασία των αναζητήσεων διακομιστών ονομάτων.
☐	8. Πρωτόκολλο	H	Μηχανισμός ασφαλείας που αποκλείει την κίνηση αν αποτύχει το VPN.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

5. Κρυπτογραφική ανάμειξη των δεδομένων για την ασφάλεια της μετάδοσης (13)

6. Αρχιτεκτονική διακομιστή που χρησιμοποιεί πτητική μνήμη για την αποθήκευση δεδομένων (9)

7. Ανεξάρτητα ελεγμένη διάταξη που επιβεβαιώνει ότι δεν αποθηκεύονται αρχεία καταγραφής (8)

8. Επιβολή ιδιωτικών ερωτημάτων DNS για την προστασία των αναζητήσεων διακομιστών ονομάτων (9)

ΚΑΘΕΤΑ

1. Μηχανισμός ασφαλείας που μπλοκάρει την κίνηση αν αποτύχει το VPN (9)

2. Επαλήθευση ότι ο χρήστης είναι αυτός που ισχυρίζεται, η οποία απαιτείται συνεχώς στο πλαίσιο μηδενικής εμπιστοσύνης (11)

3. Διαδοχική σειρά δύο κόμβων διακομιστή VPN από τους οποίους περνά η κίνηση (7)

4. Σύνολο τεχνικών κανόνων που καθορίζουν πώς πακετάρονται και στέλνονται τα δεδομένα (10)

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

5 οριζόντια: Κρυπτογραφική ανάμειξη των δεδομένων για την ασφάλεια της μετάδοσης (13 γράμματα):

6 οριζόντια: Αρχιτεκτονική διακομιστή που χρησιμοποιεί πτητική μνήμη για την αποθήκευση δεδομένων (9 γράμματα):

7 οριζόντια: Ανεξάρτητα ελεγμένη διάταξη που επιβεβαιώνει ότι δεν αποθηκεύονται αρχεία καταγραφής (8 γράμματα):

8 οριζόντια: Επιβολή ιδιωτικών ερωτημάτων DNS για την προστασία των αναζητήσεων διακομιστών ονομάτων (9 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Μηχανισμός ασφαλείας που μπλοκάρει την κίνηση αν αποτύχει το VPN (9 γράμματα):

2 κάθετα: Επαλήθευση ότι ο χρήστης είναι αυτός που ισχυρίζεται, η οποία απαιτείται συνεχώς στο πλαίσιο μηδενικής εμπιστοσύνης (11 γράμματα):

3 κάθετα: Διαδοχική σειρά δύο κόμβων διακομιστή VPN από τους οποίους περνά η κίνηση (7 γράμματα):

4 κάθετα: Σύνολο τεχνικών κανόνων που καθορίζουν πώς πακετάρονται και στέλνονται τα δεδομένα (10 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.

Ψ Α Ο Ξ Ψ Χ Σ Π Η Τ Χ Α Ο Υ Ν

Η Ι Ν Ν Ω Ξ Θ Ρ Ο Σ Μ Θ Ο Υ Τ

Σ Σ Ε Ξ Υ Τ Κ Ω Α Ε Ο Ξ Μ Λ Α

Η Α Μ Ν Υ Ζ Η Τ Ο Π Ν Χ Ψ Ι Κ

Ι Τ Γ Υ Ι Ω Φ Ο Ψ Ο Ο Κ Θ Ω Ι

Ο Σ Ε Ι Ν Α Ε Κ Θ Α Μ Σ Α Ι Ε

Π Ο Λ Φ Ε Κ Ω Ο Κ Ε Ν Κ Π Ν Ι

Ο Ρ Ε Α Ζ Ξ Κ Λ Ν Γ Η Ν Γ Δ Η

Τ Π Θ Β Α Ξ Ρ Λ Λ Ο Μ Φ Τ Θ Ψ

Υ Ζ Ω Ρ Η Χ Φ Ο Θ Ε Η Π Τ Ν Τ

Α Κ Ρ Υ Π Τ Ο Γ Ρ Α Φ Η Σ Η Κ

Τ Ρ Δ Α Λ Υ Σ Ι Δ Α Τ Σ Λ Ο Λ

Μ Σ Δ Ι Α Κ Ο Π Τ Η Σ Θ Κ Ο Θ

Ψ Ξ Λ Χ Υ Ν Ψ Π Π Β Α Λ Ο Μ Β

Λ Θ Ζ Ι Ν Ψ Β Ω Ω Ψ Β Ν Υ Χ Μ

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΤΑΥΤΟΠΟΙΗΣΗ ΑΛΥΣΙΔΑ ΜΟΝΟΜΝΗΜΗ ΠΡΟΣΤΑΣΙΑ ΔΙΑΚΟΠΤΗΣ ΕΛΕΓΜΕΝΟ
ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΠΡΩΤΟΚΟΛΛΟ

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. ΤΑΥΤΟΠΟΙΗΣΗ

B. ΑΛΥΣΙΔΑ

C. ΜΟΝΟΜΝΗΜΗ

D. ΠΡΟΣΤΑΣΙΑ

E. ΔΙΑΚΟΠΤΗΣ

F. ΕΛΕΓΜΕΝΟ

G. ΚΡΥΠΤΟΓΡΑΦΗΣΗ

H. ΠΡΩΤΟΚΟΛΛΟ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

1. Μηχανισμός ασφαλείας που μπλοκάρει την κίνηση αν αποτύχει το VPN.
2. Επιβολή ιδιωτικών ερωτημάτων DNS για την προστασία των αναζητήσεων διακομιστών ονομάτων.
3. Διαδοχική σειρά δύο κόμβων διακομιστή VPN από τους οποίους περνά η κίνηση.
4. Σύνολο τεχνικών κανόνων που καθορίζουν πώς πακετάρονται και στέλνονται τα δεδομένα.
5. Κρυπτογραφική ανάμειξη των δεδομένων για την ασφάλεια της μετάδοσης.
6. Αρχιτεκτονική διακομιστή που χρησιμοποιεί πτητική μνήμη για την αποθήκευση δεδομένων.
7. Ανεξάρτητα ελεγμένη διάταξη που επιβεβαιώνει ότι δεν αποθηκεύονται αρχεία καταγραφής.
8. Επαλήθευση ότι ο χρήστης είναι αυτός που ισχυρίζεται, η οποία απαιτείται συνεχώς στο πλαίσιο μηδενικής εμπιστοσύνης.

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. ΟΟΣΑΠΙΤΗΥΗΤ
2. ΗΜΜΟΟΝΗΜΝ
3. ΔΠΟΙΤΣΚΗΑ
4. ΟΣΑΥΡΤΗΓΗΦΚΡΠ
5. ΙΑΣΥΑΔΛ
6. ΙΣΡΣΑΠΤΑΟ
7. ΕΟΜΕΝΛΓΕ
8. ΛΤΚΟΠΟΡΟΛΩ

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	Κλειδαριές ή κλειδιά που χρησιμοποιείς κάθε μέρα			
2	Πράγματα που ένα VPN μπορεί να κρύψει			
3	Πράγματα που κάνουν ένα VPN ασφαλές			
4	Μύθοι για τα VPN			
5	Λόγοι για να χρησιμοποιείς VPN όταν ταξιδεύεις			
6	Ασφαλή μέρη στον πραγματικό κόσμο			
7	Λέξεις που σημαίνουν «προστατευμένο»			
8	Υποσχέσεις που δίνει ένας καλός πάροχος VPN			
9	Λέξεις που σχετίζονται με το απόρρητο			
10	Τύποι ελέγχου ή επιθεώρησης			
11	Λέξεις από αυτό το φύλλο εργασίας που θέλεις να θυμάσαι			
12	Πράγματα που θέλει να κλέψει ένας χάκερ			
13	Τρόποι να εντοπίσεις ένα ψεύτικο δίκτυο Wi-Fi			
14	Μέρη όπου θα χρησιμοποιούσες ένα VPN			
15	Πράγματα που μπορεί να δει ο πάροχος internet σου			

Σημείο ελέγχου 8: Μελέτες περίπτωσης VPN και δικτύου

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

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΘΩΡΑΚΙΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΥΠΟΔΟΜΗΣ



Σενάριο: Μια εταιρική τράπεζα επανασχεδιάζει την τοπολογία απομακρυσμένης πρόσβασης. Απαιτεί αρχιτεκτονική zero trust που συνδέει όλες τις συσκευές πελατών με ασφαλείς διακομιστές.

Ερώτηση συζήτησης: Ποιο είναι το κύριο όφελος της μικροτμηματοποίησης δικτύου σε ένα μοντέλο VPN Zero Trust;

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΠΡΟΣΤΑΣΙΕΣ ΔΙΑΚΟΜΙΣΤΩΝ ΜΟΝΟ RAM



Σενάριο: Ένας πάροχος VPN με έμφαση στην ασφάλεια αναβαθμίζει τους διακομιστές του ώστε η φυσική κατάσχεση διακομιστή να μην εκθέτει ιστορικά καταγραφής χρηστών.

Ερώτηση συζήτησης: Εξήγησε πώς οι διαμορφώσεις υλικού μόνο με RAM αποτρέπουν την εγκληματολογική εξαγωγή δεδομένων κατά τη φυσική κατάσχεση διακομιστών.

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

1	18	21	1	11	5	18		4	9	10	19	20	15

16	17	15	18	19	1	19	5	20	5	9		23	7	21	9	1	10	7

1	14	9	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 κάνει ένα VPN «το πιο ασφαλές»;

Συνδυασμός Zero Trust, διακομιστών μόνο RAM και ελεγμένων πρωτοκόλλων.

Q2: Τι είναι οι διακομιστές μόνο RAM;

Διακομιστές που λειτουργούν σε πτητική μνήμη, σχεδιασμένοι να μην αποθηκεύουν αρχεία καταγραφής στον δίσκο.

Q3: Τι είναι ένα VPN Zero Trust;

Ένα πλαίσιο που επαληθεύει διαρκώς κάθε αίτημα πρόσβασης και κάθε σύνδεση.

Q4: Γιατί το WireGuard θεωρείται ασφαλές;

Έχει μια μικρή, εύκολα ελέγξιμη βάση κώδικα και χρησιμοποιεί σύγχρονους κρυπτογραφικούς αλγορίθμους.

Q5: Πώς αποτρέπουν τις διαρροές DNS τα ασφαλή VPN;

Δρομολογώντας όλα τα ερωτήματα μέσω ιδιωτικών, κρυπτογραφημένων επιλυτών DNS.

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: Απαιτεί ένα ασφαλές VPN ελέγχους (audits);

Ναι, ανεξάρτητοι έλεγχοι επαληθεύουν τους ισχυρισμούς για μηδενική καταγραφή και την ασφάλεια του κώδικα.

Q7: Ποιος είναι ο ρόλος ενός kill switch;

Διακόπτει αμέσως την κίνηση δικτύου αν διακοπεί η σύνδεση VPN.

Q8: Ποια κρυπτογράφηση χρησιμοποιείται στα ασφαλή VPN;

Τα AES-256 και ChaCha20 είναι τα πρότυπα του κλάδου για την κρυπτογράφηση.

Q9: Είναι ασφαλής η δρομολόγηση Multi-Hop;

Ναι, αλυσοδένει δύο ή περισσότερους διακομιστές για να αποτρέψει την ανάλυση κίνησης.

Q10: Πώς βοηθά η υπεράκτια δικαιοδοσία;

Μπορεί να περιορίσει ποιοι νόμοι εφαρμόζονται, αλλά δεν προσφέρει απόλυτη ασυλία.

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: Πώς αποτρέπουν οι διακομιστές μόνο RAM τους κινδύνους κατάσχεσης δεδομένων;

Επειδή τρέχουν σε RAM, η αποσύνδεση από την πρίζα σβήνει τα δεδομένα που βρίσκονται στη μνήμη.

Q2: Πώς αντικαθιστά το Zero Trust την τυπική ασφάλεια περιμέτρου;

Αντιμετωπίζει κάθε πελάτη ως εχθρικό, απαιτώντας συνεχή έλεγχο ταυτότητας.

Q3: Τι κάνει τον κώδικα του WireGuard ευκολότερο να ελεγχθεί;

Ο κώδικάς του για Linux έχει λιγότερες από 4,000 γραμμές, πολύ μικρότερος από τις τυπικές στοίβες VPN. [4]

Q4: Πώς προστατεύει το DNSSEC τα ερωτήματα DNS;

Υπογράφει τις εγγραφές DNS ώστε οι επιλυτές να μπορούν να εντοπίζουν πλαστές ή παραποιημένες απαντήσεις.

Q5: Πώς περιπλέκει το Multi-Hop τη συσχέτιση της κίνησης;

Διαχωρίζοντας τις εισερχόμενες και τις εξερχόμενες IP σε διαφορετικούς παρόχους φιλοξενίας.

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: Γιατί οι δικαιοδοσίες των Five Eyes είναι επικίνδυνες για τα VPN;

Τα κράτη μέλη ανταλλάσσουν πληροφορίες και μπορεί να χρησιμοποιούν νομικές εντολές για να ζητήσουν δεδομένα χρηστών.

Q7: Πώς υλοποιείται ένα kill switch σε επίπεδο πυρήνα;

Χρησιμοποιεί κανόνες τείχους προστασίας του συστήματος (όπως iptables ή WFP) για να αποκλείει την εξερχόμενη κίνηση.

Q8: Τι είναι το προωθητικό απόρρητο (forward secrecy) στις χειραψίες VPN;

Δημιουργεί μοναδικά κλειδιά συνεδρίας ώστε οι προηγούμενες συνεδρίες να μην μπορούν να αποκρυπτογραφηθούν.

Q9: Πώς μετριάζουν τις διαρροές WebRTC τα ασφαλή VPN;

Αποκλείοντας τα αιτήματα WebRTC ή δρομολογώντας τα μέσα από τη σήραγγα.

Q10: Πώς διασφαλίζουν οι ανεξάρτητοι έλεγχοι τη συμμόρφωση με την ιδιωτικότητα;

Οι ελεγκτές διενεργούν δοκιμές διείσδυσης και επιθεωρούν τις ρυθμίσεις των διακομιστών.

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

Οι διακομιστές μόνο με RAM φορτώνουν το λειτουργικό τους σύστημα στη μνήμη κατά την εκκίνηση, οπότε τίποτα δεν παραμένει στον δίσκο μετά από επανεκκίνηση.

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Το WireGuard χρησιμοποιεί το πλαίσιο Noise με Curve25519, ChaCha20, Poly1305, BLAKE2s και HKDF. [3]

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Το Zero Trust παρέχει πρόσβαση ανά πόρο και δεν δίνει άρρητη εμπιστοσύνη με βάση την τοποθεσία στο δίκτυο (NIST SP 800-207). [1]

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Η συμμαχία πληροφοριών Five Eyes περιλαμβάνει τις ΗΠΑ, το Ηνωμένο Βασίλειο, τον Καναδά, την Αυστραλία και τη Νέα Ζηλανδία.

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Οι διαρροές WebRTC συμβαίνουν όταν τα προγράμματα περιήγησης αποκαλύπτουν την πραγματική δημόσια διεύθυνση IP του πελάτη μέσω ερωτημάτων STUN.

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Το Perfect Forward Secrecy (PFS) διασφαλίζει ότι η παραβίαση ενός μακροπρόθεσμου κλειδιού δεν εκθέτει παλαιότερα κλειδιά συνεδρίας. [3]

7. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

Η Cure53, μια εταιρεία ασφαλείας με έδρα το Βερολίνο, έχει δημοσιεύσει ελέγχους για αρκετούς παρόχους VPN.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

Οι διαρροές DNS συμβαίνουν όταν τα ερωτήματα DNS παρακάμπτουν το τούνελ VPN και πηγαίνουν στους διακομιστές ονομάτων του τοπικού παρόχου.

9. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

Τα πτητικά τσιπ RAM χρειάζονται συνεχή ηλεκτρική τροφοδοσία για να διατηρούν δεδομένα και χάνουν το περιεχόμενό τους όταν σβήσουν.

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Τα επιχειρησιακά συστήματα Zero Trust επιβάλλουν ελέγχους στάσης συσκευής προτού επιτρέψουν τη σύνδεση σε ασφαλείς πόρους. [1]

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] 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/

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 **Διακομιστής μόνο με RAM** ΜΟΝΟ RAM — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι διακομιστές μόνο με RAM δεν αποθηκεύουν αρχεία καταγραφής στον δίσκο και διαγράφουν τα δεδομένα κατά την επανεκκίνηση. Πηγή: Most Secure VPN.

2 **Ερώτηση 2** — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το WireGuard συνδυάζει μια μικρή βάση κώδικα που μπορεί να ελεγχθεί με σύγχρονους αλγορίθμους κρυπτογράφησης.

3 **Μοντέλο Zero Trust** ΜΗΔΕΝΙΚΗ ΕΜΠΙΣΤΟΣΥΝΗ — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα μοντέλα Zero Trust επαληθεύουν συνεχώς τη συμμόρφωση της συσκευής πριν από την πρόσβαση. Παραπομπή: Most Secure VPN.

4 **Προστασία DNS** ΠΡΟΣΤΑΣΙΑ DNS — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η προστασία από διαρροές DNS δρομολογεί τα ερωτήματα αναζήτησης μέσω ιδιωτικών resolver. Παραπομπή: Most Secure VPN.

5 **Τούνελ Multi-Hop** MULTI-HOP — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η δρομολόγηση Multi-Hop αλυσιδώνει δύο ξεχωριστούς κόμβους διακομιστών διαδοχικά. Παραπομπή: Most Secure VPN.

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 **Διακομιστής μόνο με RAM** MONO RAM — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ο εξοπλισμός διακομιστή μόνο με RAM δεν γράφει δεδομένα στον δίσκο και διαγράφεται κατά την επανεκκίνηση. Πηγή: Most Secure VPN.

7 **Ταχύτητα WireGuard** WIREGUARD — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το WireGuard χρησιμοποιεί σύγχρονη κρυπτογραφία που αποφεύγει τα σημεία συμφόρησης επεξεργασίας. Παραπομπή: Most Secure VPN.

8 **Kill switch** ΔΙΑΚΟΠΤΗΣ ΑΣΦΑΛΕΙΑΣ — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ένας kill switch αποκλείει όλη την κίνηση αν διακοπεί η σύνδεση VPN. Παραπομπή: Most Secure VPN.

9 **Έλεγχοι από τρίτους** ΟΙ ΕΛΕΓΧΟΙ ΕΙΝΑΙ ΖΩΤΙΚΟΙ — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι έλεγχοι από τρίτους είναι απαραίτητοι για την επαλήθευση των ισχυρισμών ιδιωτικότητας των εταιρειών. Παραπομπή: Most Secure VPN.

10 **Ερώτηση 10** — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το Zero Trust δεν παρέχει σιωπηρή εμπιστοσύνη με βάση την τοποθεσία στο δίκτυο.

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. Zero Trust	E 2. Multi-Hop	F 3. Διακομιστής μόνο με RAM	G 4. Προστασία DNS
H 5. Kill switch	A 6. Σύστημα με έλεγχο	B 7. Κρυπτογράφηση	D 8. Πρωτόκολλο

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ZERO TRUST	2 MULTI-HOP	3 ΜΟΝΟ ΜΝΗΜΗ	4 ΠΡΟΣΤΑΣΙΑ
5 ΔΙΑΚΟΠΤΗΣ	6 ΕΛΕΓΜΕΝΟ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 E – ΔΙΑΚΟΠΤΗΣ	2 D – ΠΡΟΣΤΑΣΙΑ	3 B – ΑΛΥΣΙΔΑ	4 H – ΠΡΩΤΟΚΟΛΛΟ
5 G – ΚΡΥΠΤΟΓΡΑΦΗΣΗ	6 C – ΜΟΝΟΜΝΗΜΗ	7 F – ΕΛΕΓΜΕΝΟ	8 A – ΤΑΥΤΟΠΟΙΗΣΗ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους Zero Trust, Multi-Hop και Διακομιστής μόνο με RAM 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

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

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ

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

ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

5 οριζόντια: ΚΡΥΠΤΟΓΡΑΦΗΣΗ Κρυπτογραφική ανάμειξη των δεδομένων για την ασφάλεια της μετάδοσης (13 γράμματα)

6 οριζόντια: ΜΟΝΟΜΝΗΜΗ Αρχιτεκτονική διακομιστή που χρησιμοποιεί πτητική μνήμη για την αποθήκευση δεδομένων (9 γράμματα)

7 οριζόντια: ΕΛΕΓΜΕΝΟ Ανεξάρτητα ελεγμένη διάταξη που επιβεβαιώνει ότι δεν αποθηκεύονται αρχεία καταγραφής (8 γράμματα)

8 οριζόντια: ΠΡΟΣΤΑΣΙΑ Επιβολή ιδιωτικών ερωτημάτων DNS για την προστασία των αναζητήσεων διακομιστών ονομάτων (9 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΔΙΑΚΟΠΤΗΣ Μηχανισμός ασφαλείας που μπλοκάρει την κίνηση αν αποτύχει το VPN (9 γράμματα)

2 κάθετα: ΤΑΥΤΟΠΟΙΗΣΗ Επαλήθευση ότι ο χρήστης είναι αυτός που ισχυρίζεται, η οποία απαιτείται συνεχώς στο πλαίσιο μηδενικής εμπιστοσύνης (11 γράμματα)

3 κάθετα: ΑΛΥΣΙΔΑ Διαδοχική σειρά δύο κόμβων διακομιστή VPN από τους οποίους περνά η κίνηση (7 γράμματα)

4 κάθετα: ΠΡΩΤΟΚΟΛΛΟ Σύνολο τεχνικών κανόνων που καθορίζουν πώς πακετάρονται και στέλνονται τα δεδομένα (10 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

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

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΟΟΣΑΠΙΤΗΥΗΤ — **ΤΑΥΤΟΠΟΙΗΣΗ**
2. ΗΜΜΟΟΝΗΜΝ — **ΜΟΝΟΜΝΗΜΗ**
3. ΔΠΟΙΤΣΚΗΑ — **ΔΙΑΚΟΠΤΗΣ**
4. ΟΣΑΥΡΤΗΓΗΦΚΡΠ — **ΚΡΥΠΤΟΓΡΑΦΗΣΗ**
5. ΙΑΣΥΑΔΛ — **ΑΛΥΣΙΔΑ**
6. ΙΣΡΣΑΠΤΑΟ — **ΠΡΟΣΤΑΣΙΑ**
7. ΕΟΜΕΝΛΓΕ — **ΕΛΕΓΜΕΝΟ**
8. ΛΤΚΟΠΟΡΟΛΩ — **ΠΡΩΤΟΚΟΛΛΟ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΑΣΦΑΛΕΣ ΔΙΚΤΥΟ ΠΡΟΣΤΑΤΕΥΕΙ ΨΗΦΙΑΚΗ ΑΞΙΑ"

Λύσεις των μελετών περίπτωσης

A ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΘΩΡΑΚΙΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΥΠΟΔΟΜΗΣ

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Μια εταιρική τράπεζα επανασχεδιάζει την τοπολογία απομακρυσμένης πρόσβασης. Χρειάζεται αρχιτεκτονική μηδενικής εμπιστοσύνης που συνδέει όλες τις συσκευές πελατών με ασφαλείς διακομιστές.
- Προτεινόμενη στρατηγική και λύση: Οδηγίες βαθμολόγησης: Εξήγησε ότι η μικροτμηματοποίηση περιορίζει την πρόσβαση σε συγκεκριμένους πόρους, αποτρέποντας την πλευρική κίνηση απειλών αν παραβιαστεί μια συσκευή.

B ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΠΡΟΣΤΑΣΙΕΣ ΔΙΑΚΟΜΙΣΤΩΝ ΜΟΝΟ RAM

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένας πάροχος VPN με επίκεντρο την ασφάλεια αναβαθμίζει τους διακομιστές του ώστε η φυσική κατάσχεση διακομιστή να μην εκθέτει το ιστορικό αρχείων καταγραφής χρηστών.
- Προτεινόμενη στρατηγική και λύση: Οδηγίες βαθμολόγησης: Περίγραψε ότι οι διακομιστές μόνο RAM δεν έχουν φυσική αποθήκευση σε δίσκο. Η διακοπή ρεύματος διαγράφει αυτόματα όλα τα προσωρινά δεδομένα στην πτητική μνήμη.