Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

VPN απομακρυσμένης πρόσβασης

Ασφάλιση τερματικών απομακρυσμένου εργατικού δυναμικού, πολυπαραγοντική ταυτοποίηση και ρυθμίσεις τούνελ IPsec.

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ ΓΙΑ VPN ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΠΡΟΣΒΑΣΗΣ

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 δίκτυα VPN απομακρυσμένης πρόσβασης. Θα εξερευνήσεις σήραγγες πελάτη-προς-τοποθεσία, συνδέσεις πολλαπλών παραγόντων, ελέγχους κατάστασης τερματικών, όρια εύρους ζώνης και έλεγχο ασφάλειας μέσω syslog.

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/kalytero-vpn-gia-epicheiriseis/apomakrysmenh-prosvash/

Η πορεία μάθησής σου: VPN απομακρυσμένης πρόσβασης

- Ασφαλή τερματικά απομακρυσμένου εργατικού δυναμικού που έχουν πρόσβαση σε κόμβους τοπικού δικτύου.
- Ρύθμισε πολιτικές πολυπαραγοντικής ταυτοποίησης για απομακρυσμένες συνδέσεις.
- Ρύθμισε διαμορφώσεις IPsec και OpenVPN client-to-site.
- Έλεγξε τα αρχεία καταγραφής απομακρυσμένων συνδέσεων για παραβιάσεις ελέγχου πρόσβασης.
- Εφάρμοσε ελέγχους κατάστασης συσκευής πριν παραχωρήσεις συνδέσεις δικτύου.
- Βελτιστοποίησε τη διεκπεραιωτική ικανότητα του διακομιστή για να αποφύγεις το στένεμα του εύρους ζώνης στην τηλεργασία.

ΟΔΗΓΙΕΣ ΓΙΑ VPN ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΠΡΟΣΒΑΣΗΣ

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 στους ελέγχους ασφαλούς κατάστασης (posture checks) και στις συνδέσεις πολλαπλών παραγόντων. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΣΗΡΑΓΓΕΣ CLIENT-TO-SITE ΚΑΙ ΣΥΜΜΟΡΦΩΣΗ ΤΕΛΙΚΩΝ ΣΗΜΕΙΩΝ (ΕΙΣΑΓΩΓΗ)

Τα VPN απομακρυσμένης πρόσβασης δημιουργούν ασφαλείς σήραγγες πελάτη-προς-ιστότοπο για υπαλλήλους εκτός γραφείου. Η ασφάλεια αυτών των συνδέσεων απαιτεί επιβολή συνδέσεων με έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA), ελέγχους συμμόρφωσης κατάστασης των τερματικών και έλεγχο των αρχείων καταγραφής μέσω κεντρικών συλλεκτών syslog.

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **Ποιο πρότυπο ταυτοποίησης πρέπει να επιβάλλουν οι πύλες VPN απομακρυσμένης πρόσβασης;**

- A) Πολλαπλών παραγόντων
- B) Ένας παράγοντας
- C) Χωρίς κρυπτογράφηση
- D) Τοπικός επισκέπτης

2. **Ποιο πρωτόκολλο είναι το πρότυπο για την ασφάλιση συνδέσεων πελάτη προς τοποθεσία (client-to-site) στην απομακρυσμένη εργασία;**

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3. **Ποιος έλεγχος επαληθεύει αν ένας απομακρυσμένος φορητός υπολογιστής είναι καθαρός πριν συνδεθεί;**

- A) Έλεγχος κατάστασης ασφαλείας (posture check)
- B) Δοκιμή ταχύτητας
- C) Δοκιμή ping
- D) Αριθμός μνήμης

4. **Πού αποθηκεύονται τα αρχεία καταγραφής συνδέσεων των απομακρυσμένων εργαζομένων για έλεγχο ασφάλειας;**

- A) Διακομιστής Syslog
- B) Κλειδί μητρώου
- C) Μνήμη πελάτη
- D) Πρόγραμμα περιήγησης

5. **Ποιο πρόβλημα παρουσιάζεται όταν ο αριθμός των απομακρυσμένων εργαζομένων υπερβαίνει τη χωρητικότητα εύρους ζώνης της πύλης;**

- A) Περιορισμός εύρους ζώνης
- B) Διαρροή DNS
- C) Επιτυχής χειραψία
- D) Έκθεση IP

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων προσθέτει ένα δεύτερο διακριτικό επικύρωσης για την ασφάλεια των απομακρυσμένων συνδέσεων.

Σωστό Λάθος

7 Ερώτηση 7

7. Οι έλεγχοι στάσης ασφαλείας επιτρέπουν σε απομακρυσμένες συσκευές με απενεργοποιημένα τείχη προστασίας να έχουν πρόσβαση σε ιδιωτικούς διακομιστές.

Σωστό Λάθος

8 Ερώτηση 8

8. Τα αρχεία καταγραφής των VPN απομακρυσμένης πρόσβασης είναι ουσιώδη για τον εντοπισμό μη εξουσιοδοτημένης εισόδου στο εταιρικό δίκτυο.

Σωστό Λάθος

9 Ερώτηση 9

9. Το OpenVPN και το IPsec είναι παλαιά πρωτόκολλα που δεν κρυπτογραφούν τα δεδομένα των απομακρυσμένων πελατών.

Σωστό Λάθος

10 Ερώτηση 10

10. Η στένωση του εύρους ζώνης της πύλης συμβαίνει όταν η απομακρυσμένη κίνηση υπερβαίνει τη χωρητικότητα της κάρτας σύνδεσης.

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. Για την προστασία των εταιρικών πυλών, οι απομακρυσμένες συνδέσεις πρέπει να απαιτούν ταυτοποίηση στην οποία χρειάζονται πολλαπλοί _____ .

2. Οι απομακρυσμένοι πελάτες κρυπτογραφούν τα δεδομένα των τούνελ με τυπικά πρωτόκολλα όπως το _____ .

3. Οι συσκευές πρέπει να περάσουν έλεγχο ασφαλείας ως προς την _____ τους πριν συνδεθούν στο δίκτυο.

4. Τα ελεγχόμενα αρχεία καταγραφής εισόδου αποστέλλονται συνεχώς σε έναν κεντρικό διακομιστή _____ .

5. Η μεγάλη κίνηση τις ώρες εργασίας μπορεί να προκαλέσει συμφόρηση στο _____ της πύλης.

6. Οι οδηγοί εικονικών προσαρμογέων διαχειρίζονται τη _____ από πελάτη προς τοποθεσία στα Windows και macOS.

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΕΥΡΟΣ ΖΩΝΗΣ ΚΑΤΑΣΤΑΣΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΠΑΡΑΓΟΝΤΕΣ ΣΗΡΑΓΓΟΠΟΙΗΣΗ ΤΕΙΧΟΣ OPENVPN SYSLOG

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση βασικών εννοιών

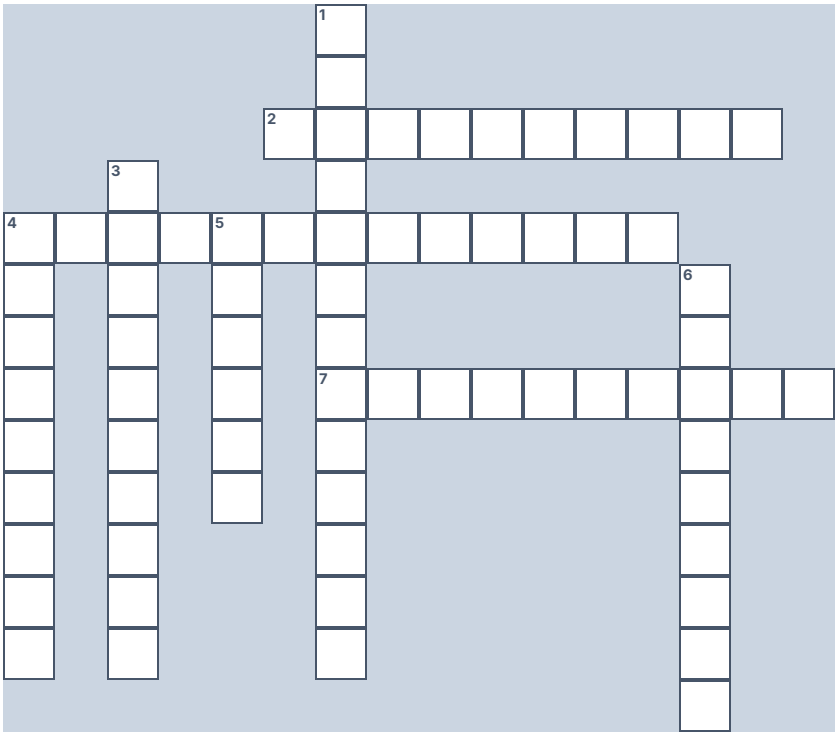
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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

☐	1. ΠΟΛΛΑΠΛΩΝ ΠΑΡΑΓΟΝΤΩΝ	**A**	Ενθυλάκωση δεδομένων σε μια ασφαλή διαδρομή.
☐	2. OPENVPN	**B**	Κεντρικός συλλέκτης αρχείων καταγραφής ασφαλείας.
☐	3. ΣΤΑΣΗ ΑΣΦΑΛΕΙΑΣ	**C**	Όριο χωρητικότητας δεδομένων δικτύου.
☐	4. SYSLOG	**D**	Τυπικό πρωτόκολλο client-to-site.
☐	5. ΕΥΡΟΣ ΖΩΝΗΣ	**E**	Επικύρωση υγείας απομακρυσμένης συσκευής.
☐	6. ΚΡΥΠΤΟΓΡΑΦΗΣΗ	**F**	Κανόνες συστήματος φιλτραρίσματος κίνησης.
☐	7. ΤΟΥΝΕΛΟΠΟΙΗΣΗ	**G**	Κρυπτογραφικό ανακάτεμα πακέτων.
☐	8. ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ	**H**	Ασφάλεια σύνδεσης που απαιτεί επιπλέον διακριτικά.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

2. Τυπικό σύνολο κανόνων για σύνδεση πελάτη προς τοποθεσία (10)

4. Κρυπτογραφική αλλοίωση των πακέτων (13)

7. Ασφάλεια σύνδεσης που απαιτεί επιπλέον διακριτικά (10)

ΚΑΘΕΤΑ

1. Ενθυλάκωση δεδομένων σε ασφαλή διαδρομή (13)

3. Όριο χωρητικότητας δεδομένων του δικτύου (10)

4. Συγκέντρωση των αρχείων ασφαλείας σε έναν κεντρικό συλλέκτη (9)

5. Κανόνες του συστήματος φιλτραρίσματος της κίνησης (τείχος προστασίας) (6)

6. Επικύρωση της υγείας της απομακρυσμένης συσκευής (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

2 οριζόντια: Τυπικό σύνολο κανόνων για σύνδεση πελάτη προς τοποθεσία (10 γράμματα):

4 οριζόντια: Κρυπτογραφική αλλοίωση των πακέτων (13 γράμματα):

7 οριζόντια: Ασφάλεια σύνδεσης που απαιτεί επιπλέον διακριτικά (10 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Ενθυλάκωση δεδομένων σε ασφαλή διαδρομή (13 γράμματα):

3 κάθετα: Όριο χωρητικότητας δεδομένων του δικτύου (10 γράμματα):

4 κάθετα: Συγκέντρωση των αρχείων ασφαλείας σε έναν κεντρικό συλλέκτη (9 γράμματα):

5 κάθετα: Κανόνες του συστήματος φιλτραρίσματος της κίνησης (τείχος προστασίας) (6 γράμματα):

6 κάθετα: Επικύρωση της υγείας της απομακρυσμένης συσκευής (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.

Η Χ Σ Η Σ Τ Χ Α Ο Υ Ν Ν Ω Ξ Θ

Σ Ο Σ Θ Ο Ε Υ Τ Ξ Υ Τ Κ Α Ε Ξ

Η Μ Λ Α Κ Α Τ Α Σ Τ Α Σ Η Ν Υ

Ι Ζ Η Ο Π Χ Ψ Ν Ι Σ Κ Υ Ι Ω Φ

Ο Ψ Ο Κ Θ Ω Ι Ι Ο Ν Ο Α Ε Θ Α

Π Σ Α Ι Ε Φ Ε Κ Ω Γ Κ Χ Ε Κ Π

Ο Ν Ι Α Ζ Ξ Κ Ν Γ Ν Α Γ Ι Δ Η

Γ Θ Β Α Ξ Ρ Λ Ο Φ Τ Θ Ρ Ψ Ε Ζ

Γ Ω Ρ Η Χ Φ Θ Ε Π Τ Ν Τ Α Κ Τ

Α Ρ Σ Η Ν Ω Ζ Σ Ο Ρ Υ Ε Δ Π Τ

Ρ Κ Ρ Υ Π Τ Ο Γ Ρ Α Φ Η Σ Η Σ

Η Λ Ο Κ Α Τ Α Γ Ρ Α Φ Η Λ Μ Σ

Σ Θ Π Ρ Ω Τ Ο Κ Ο Λ Λ Ο 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

ΠΑΡΑΓΟΝΤΕΣ ΠΡΩΤΟΚΟΛΛΟ ΚΑΤΑΣΤΑΣΗ ΚΑΤΑΓΡΑΦΗ ΕΥΡΟΣΖΩΝΗΣ
ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΣΗΡΑΓΓΟΠΟΙΗΣΗ ΤΕΙΧΟΣ

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. ΠΑΡΑΓΟΝΤΕΣ**
- **B. ΠΡΩΤΟΚΟΛΛΟ**
- **C. ΚΑΤΑΣΤΑΣΗ**
- **D. ΚΑΤΑΓΡΑΦΗ**
- **E. ΕΥΡΟΖΩΝΗΣ**
- **F. ΚΡΥΠΤΟΓΡΑΦΗΣΗ**
- **G. ΣΗΡΑΓΓΟΠΟΙΗΣΗ**
- **H. ΤΕΙΧΟΣ**

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

1. Συγκέντρωση των αρχείων ασφαλείας σε έναν κεντρικό συλλέκτη.
2. Κανόνες του συστήματος φιλτραρίσματος της κίνησης (τείχος προστασίας).
3. Ενθυλάκωση δεδομένων σε ασφαλή διαδρομή.
4. Κρυπτογραφική αλλοίωση των πακέτων.
5. Τυπικό σύνολο κανόνων για σύνδεση πελάτη προς τοποθεσία.
6. Όριο χωρητικότητας δεδομένων του δικτύου.
7. Επικύρωση της υγείας της απομακρυσμένης συσκευής.
8. Ασφάλεια σύνδεσης που απαιτεί επιπλέον διακριτικά.

Σημείο ελέγχου 7: Πρόκληση ανακατεμένων λέξεων

Αποκωδικοποίησε τα γράμματα παρακάτω για να αποκαλύψεις βασικές έννοιες και όρους της μεσιτείας domain. Γράψε τις απαντήσεις σου στα διαθέσιμα πλαίσια εισαγωγής.

1. ΕΝΟΓΑΠΤΣΑΡ
2. ΗΚΣΑΑΤΑΣΤ
3. ΕΖΗΩΥΣΣΟΝΡ
4. ΓΣΟΡΠΓΗΟΗΙΣΗΑ
5. ΛΚΟΡΤΟΟΠΛΩ
6. ΦΑΑΑΡΚΓΗΤ
7. ΦΗΡΟΚΡΑΤΗΣ ΥΓΠ
8. ΙΣΤΟΧΕ

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	**Μύθοι για τα VPN**			
2	**Λέξεις που περιγράφουν το Zero Trust**			
3	**Προγράμματα γραφείου που γνωρίζεις**			
4	**Κανόνες για ασφαλή τηλεργασία**			
5	**Πράγματα που μπορεί να δει ο πάροχος internet σου**			
6	**Υπηρεσίες VPN που γνωρίζεις**			
7	**Μέρη από όπου εργάζονται οι εργαζόμενοι**			
8	**Εργαλεία που χρησιμοποιεί μια εταιρεία καθημερινά**			
9	**Ρόλοι σε ένα τμήμα πληροφορικής**			
10	**Συσκευές που μπορεί να έχει ένας εργαζόμενος**			
11	**Δεδομένα που πρέπει να προστατεύει μια εταιρεία**			
12	**Πράγματα που κάνεις μετά από μια παραβίαση ασφαλείας**			
13	**Πράγματα που μπορούν να διαταράξουν μια βιντεοσύσκεψη**			
14	**Τρόποι να συνδέεσαι με ασφάλεια**			
15	**Λόγοι για να δώσεις VPN στους εργαζομένους**			

Σημείο ελέγχου 8: Μελέτες περίπτωσης VPN και δικτύου

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

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΕΠΙΒΟΛΗ MFA



Σενάριο: Ένας επιχειρηματικός αναλυτής προσπαθεί να συνδεθεί στην εταιρική βάση δεδομένων ενώ εργάζεται εξ αποστάσεως. Εισάγει το σωστό όνομα χρήστη και κωδικό πρόσβασης, αλλά η πύλη VPN μπλοκάρει την πρόσβαση και απαιτεί κωδικό από φυσικό διακριτικό.

Ερώτηση συζήτησης: Ποια πολιτική ασφάλειας επιβάλλει αυτό το βήμα διπλής επαλήθευσης;

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΣΥΜΜΟΡΦΩΣΗ ΣΤΑΣΗΣ ΑΣΦΑΛΕΙΑΣ



Σενάριο: Ένας εξωτερικός συνεργάτης συνδέει το προσωπικό του laptop στο απομακρυσμένο εταιρικό δίκτυο. Ο πελάτης VPN διακόπτει αμέσως τη σύνδεση, ενημερώνοντας τον χρήστη ότι οι ορισμοί του antivirus είναι παλιοί.

Ερώτηση συζήτησης: Ποιος εξειδικευμένος έλεγχος της πύλης VPN μπλόκαρε αυτή την προσπάθεια σύνδεσης;

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

7	1	16	15	12	1	10	17	20	18	12	5	13	7

16	17	15	18	2	1	18	7	16	17	15	18	19	1	19	5	20	5	9

18	20	18	10	5	20	5	18

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 ένα VPN απομακρυσμένης πρόσβασης;

Μια ασφαλής μέθοδος σύνδεσης που επιτρέπει στους υπαλλήλους που εργάζονται εκτός γραφείου να συνδέονται απευθείας με ιδιωτικούς εταιρικούς διακομιστές.

Q2: Γιατί η σύνδεση client-to-site διαφέρει από τη σύνδεση site-to-site;

Το client-to-site συνδέει μεμονωμένες συσκευές χρηστών, ενώ το site-to-site συνδέει ολόκληρους φυσικούς χώρους γραφείων.

Q3: Τι είναι ο έλεγχος κατάστασης συσκευής (device posture check);

Μια σάρωση που ελέγχει την κατάσταση ασφαλείας μιας απομακρυσμένης συσκευής (antivirus, επίπεδο ενημερώσεων του λειτουργικού) πριν επιτραπεί η πρόσβαση.

Q4: Γιατί χρησιμοποιείται το OpenVPN για απομακρυσμένη πρόσβαση;

Λόγω του ισχυρού πρωτοκόλλου ασφαλείας, της συμβατότητας μεταξύ πλατφορμών και της ικανότητας διαχείρισης μεμονωμένων συνδέσεων.

Q5: Πώς προστατεύει το MFA την απομακρυσμένη πρόσβαση;

Προσθέτει ένα δευτερεύον διακριτικό επαλήθευσης, εμποδίζοντας την πρόσβαση ακόμη και αν διαρρεύσουν ή κλαπούν οι κωδικοί πρόσβασης των υπαλλήλων.

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: Τι είναι ένας διακομιστής syslog;

Ένα κεντρικό αποθετήριο αρχείων καταγραφής που αποθηκεύει συμβάντα σύνδεσης, συνδέσεις χρηστών και ειδοποιήσεις συστήματος για ελέγχους συμμόρφωσης.

Q7: Τι προκαλεί την πνιγμονή του εύρους ζώνης;

Όταν οι συνολικές απαιτήσεις εύρους ζώνης των απομακρυσμένων εργαζομένων υπερβαίνουν το όριο ταχύτητας διαδικτύου της εταιρικής πύλης.

Q8: Μπορώ να συνδέσω τον οικιακό μου υπολογιστή σε VPN εργασίας;

Μόνο εφόσον η συσκευή περνά τους ελέγχους ασφάλειας της εταιρείας και έχει εγκριθεί από τους διαχειριστές πληροφορικής.

Q9: Τι είναι η ενθυλάκωση δικτύου (network encapsulation);

Η περιτύλιξη των πακέτων δεδομένων κατά τη μετάδοση μέσα σε κρυπτογραφημένες κεφαλίδες πρωτοκόλλου για την ασφάλεια της μετάδοσης.

Q10: Πώς βελτιστοποιεί η διαχωρισμένη διοχέτευση την απομακρυσμένη πρόσβαση;

Επιτρέπει στους υπαλλήλους να χρησιμοποιούν τον τοπικό ISP τους για την τυπική περιήγηση, ενώ τα αρχεία που σχετίζονται με την εργασία δρομολογούνται μέσω του 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: Πώς ενισχύει ο έλεγχος ταυτότητας βάσει πιστοποιητικών την απομακρυσμένη πρόσβαση;

Δεσμεύει τα δικαιώματα σύνδεσης σε προεγκατεστημένα τοπικά ψηφιακά πιστοποιητικά, αποκλείοντας μη διαχειριζόμενες ή μη εξουσιοδοτημένες συσκευές.

Q2: Ποιος είναι ο κίνδυνος ασφαλείας της διαχωρισμένης διοχέτευσης για την τηλεργασία;

Δημιουργεί μια πιθανή γέφυρα όπου μια παραβιασμένη τοπική συσκευή μπορεί να δρομολογήσει εξωτερικές απειλές στο ιδιωτικό δίκτυο.

Q3: Πώς ελέγχουν οι έλεγχοι κατάστασης (posture checks) τις ρυθμίσεις μητρώου;

Ο πελάτης VPN εκτελεί τοπικά σενάρια που ερωτούν διαδρομές μητρώου για να επαληθεύσουν αν το εταιρικό λογισμικό ασφαλείας εκτελείται ενεργά.

Q4: Γιατί τα syslog χρησιμοποιούν από προεπιλογή τη θύρα UDP 514;

Για γρήγορη μετάδοση αρχείων καταγραφής με ελάχιστη επιβάρυνση, αν και οι ασφαλείς διαμορφώσεις πλέον επιβάλλουν ενθυλάκωση TLS πάνω από TCP.

Q5: Πώς επιλύουν οι εταιρείες τα σημεία συμφόρησης εύρους ζώνης της πύλης;

Εφαρμόζοντας load balancers και κατανέμοντας την απομακρυσμένη κίνηση σε περιφερειακούς κόμβους διακομιστών.

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: Ποια είναι η λειτουργία των εικονικών προσαρμογέων TAP/TUN σε απομακρυσμένους πελάτες;

Λειτουργούν ως εικονικές κάρτες δικτύου, δρομολογώντας την κίνηση TCP/IP σε επίπεδο συσκευής απευθείας στην κρυπτογραφημένη σήραγγα VPN.

Q7: Πώς υποστηρίζει το IKEv2 MOBIKE την κινητικότητα του απομακρυσμένου εργατικού δυναμικού;

Ενημερώνει δυναμικά τις αντιστοιχίσεις διευθύνσεων IP, διατηρώντας το VPN ενεργό καθώς ο χρήστης μετακινείται μεταξύ Wi-Fi και δεδομένων κινητής.

Q8: Ποια είναι η διαφορά μεταξύ δρομολόγησης split και πλήρους σήραγγας;

Η πλήρης δρομολόγηση αναγκάζει όλη την κίνηση διαδικτύου της συσκευής να περνά μέσω του VPN, ενώ η διαχωρισμένη δρομολόγηση στέλνει μόνο τις IP προορισμού της εταιρείας.

Q9: Πώς χειρίζονται οι συσκευές NAT τις απομακρυσμένες συνδέσεις VPN;

Αντιστοιχίζοντας εύρη τοπικών θυρών σε δημόσιες διευθύνσεις IP πύλης για τη δρομολόγηση των κρυπτογραφημένων πακέτων δεδομένων που επιστρέφουν.

Q10: Ποια πρότυπα συμμόρφωσης επιβάλλουν έλεγχο απομακρυσμένης πρόσβασης;

Πρότυπα όπως τα HIPAA, SOC 2 και PCI DSS απαιτούν καταγραφή και παρακολούθηση όλων των συνεδριών απομακρυσμένης σύνδεσης.

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

Τα VPN απομακρυσμένης πρόσβασης δημιουργούν ασφαλείς σήραγγες πελάτη-προς-ιστότοπο για εργαζομένους εκτός γραφείου.

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων απαιτείται από κανόνες συμμόρφωσης για την προστασία απομακρυσμένων επαγγελματικών πυλών.

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Οι έλεγχοι στάσης ασφαλείας επαληθεύουν τις τοπικές ρυθμίσεις ασφαλείας του πελάτη πριν χορηγηθεί πρόσβαση στο ιδιωτικό δίκτυο.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Οι διακομιστές Syslog συγκεντρώνουν αρχεία καταγραφής συνδέσεων για έλεγχο και εντοπισμό απόπειρων μη εξουσιοδοτημένης πρόσβασης.

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Οι στενώσεις του εύρους ζώνης της πύλης συμβαίνουν όταν η συνολική απομακρυσμένη ζήτηση κίνησης υπερβαίνει τα όρια διαδικτύου του διακομιστή.

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Οι εικονικοί προσαρμογείς δικτύου ενθυλακώνουν τα ερωτήματα δικτύου του λειτουργικού συστήματος μέσα σε ασφαλή πρωτόκολλα.

7. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

Η υποστήριξη MOBIKE επιτρέπει σε απομακρυσμένους πελάτες να αλλάζουν δίκτυο χωρίς να πέφτει το τούνελ VPN.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

Η δρομολόγηση πλήρους σήραγγας ασφαλίζει όλη την κίνηση διαδικτύου των εργαζομένων αλλά αυξάνει το φορτίο της εταιρικής πύλης.

9. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

Η πιστοποίηση με πιστοποιητικό συνδέει την εξουσιοδότηση σύνδεσης VPN απευθείας με υλικό που διαχειρίζεται η εταιρεία.

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Πλαίσια όπως το SOC 2 και το PCI DSS απαιτούν καταγραφή και παρακολούθηση των συνεδριών απομακρυσμένης πρόσβασης.

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] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.

https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.

https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.

https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.

https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).

https://www.rfc-editor.org/rfc/rfc4555

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 **Διακριτικά σύνδεσης** ΑΣΦΑΛΕΙΑ MFA **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων επιβάλλει δευτερεύουσα επαλήθευση στις συνδέσεις. Παραπομπή: MFA Implementation.

2 **Τούνελ OpenVPN** ΠΕΛΑΤΗΣ ΠΡΟΣ ΙΣΤΟΤΟΠΟ **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το OpenVPN είναι πρότυπο πρωτόκολλο για την ασφάλιση τούνελ από πελάτη προς ιστότοπο. Παραπομπή: OpenVPN Client.

3 **Έλεγχοι στάσης ασφαλείας** ΕΛΕΓΧΟΣ ΣΥΣΚΕΥΗΣ **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι έλεγχοι στάσης ασφαλείας σαρώνουν τα τερματικά για ενεργά τείχη προστασίας και εργαλεία antivirus. Παραπομπή: Posture Compliance.

4 **Συγκεντρωτής αρχείων καταγραφής** ΔΙΑΚΟΜΙΣΤΗΣ SYSLOG **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι διακομιστές Syslog συλλέγουν αρχεία καταγραφής συμβάντων ασφαλείας για την παρακολούθηση παραβιάσεων πρόσβασης. Παραπομπή: Syslog Standard.

5 **Υπερχείλιση κάρτας** ΣΤΕΝΟΠΟΙΗΣΗ ΠΥΛΗΣ **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η στένωση του εύρους ζώνης της πύλης συμβαίνει όταν η κίνηση των χρηστών υπερβαίνει τα όρια του διακομιστή. Παραπομπή: Capacity Planning.

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 **Διακριτικά σύνδεσης** ΕΛΕΓΧΟΙ MFA — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων επιβάλλει δευτερεύουσα επαλήθευση στις συνδέσεις. Παραπομπή: MFA Implementation.

7 **Ερώτηση 7** — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι έλεγχοι στάσης αποκλείουν συσκευές των οποίων το τείχος προστασίας ή το antivirus είναι απενεργοποιημένο, οπότε οι συσκευές αυτές απορρίπτονται.

8 **Συγκεντρωτής αρχείων καταγραφής** ΔΙΑΚΟΜΙΣΤΗΣ SYSLOG — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι διακομιστές Syslog συλλέγουν αρχεία καταγραφής συμβάντων ασφαλείας για την παρακολούθηση παραβιάσεων πρόσβασης. Παραπομπή: Syslog Standard.

9 **Ερώτηση 9** — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα OpenVPN και IPsec είναι τρέχοντα πρωτόκολλα που κρυπτογραφούν την κίνηση απομακρυσμένων πελατών.

10 **Υπερχείλιση κάρτας** ΣΤΕΝΟΠΟΙΗΣΗ ΠΥΛΗΣ — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η στένωση του εύρους ζώνης της πύλης συμβαίνει όταν η κίνηση των χρηστών υπερβαίνει τα όρια του διακομιστή. Παραπομπή: Capacity Planning.

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

H 1. ΠΟΛΛΑΠΛΩΝ ΠΑΡΑΓΟΝΤΩΝ	D 2. OPENVPN	E 3. ΣΤΑΣΗ ΑΣΦΑΛΕΙΑΣ	B 4. SYSLOG
C 5. ΕΥΡΟΣ ΖΩΝΗΣ	G 6. ΚΡΥΠΤΟΓΡΑΦΗΣΗ	A 7. ΤΟΥΝΕΛΟΠΟΙΗΣΗ	F 8. ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΠΑΡΑΓΟΝΤΕΣ	2 OPENVPN	3 ΚΑΤΑΣΤΑΣΗ	4 SYSLOG
5 ΕΥΡΟΣ ΖΩΝΗΣ	6 ΣΗΡΑΓΓΟΠΟΙΗΣΗ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 D – ΚΑΤΑΓΡΑΦΗ	2 H – ΤΕΙΧΟΣ	3 G – ΣΗΡΑΓΓΟΠΟΙΗΣΗ	4 F – ΚΡΥΠΤΟΓΡΑΦΗΣΗ
5 B – ΠΡΩΤΟΚΟΛΛΟ	6 E – ΕΥΡΟΣΖΩΝΗΣ	7 C – ΚΑΤΑΣΤΑΣΗ	8 A – ΠΑΡΑΓΟΝΤΕΣ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους ΠΟΛΛΑΠΛΩΝ ΠΑΡΑΓΟΝΤΩΝ, OPENVPN και ΣΤΑΣΗ ΑΣΦΑΛΕΙΑΣ 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	Χ	Σ	Η	Σ	Τ	Χ	Α	Ο	Υ	Ν	Ν	Ω	Ξ	Θ
Σ	Ο	Σ	Θ	Ο	Ε	Υ	Τ	Ξ	Υ	Τ	Κ	Α	Ε	Ξ
Η	Μ	Λ	Α	Κ	Α	Τ	Α	Σ	Τ	Α	Σ	Η	Ν	Υ
Ι	Ζ	Η	Ο	Π	Χ	Ψ	Ν	Ι	Σ	Κ	Υ	Ι	Ω	Φ
Ο	Ψ	Ο	Κ	Θ	Ω	Ι	Ι	Ο	Ν	Ο	Α	Ε	Θ	Α
Π	Σ	Α	Ι	Ε	Φ	Ε	Κ	Ω	Γ	Κ	Χ	Ε	Κ	Π
Ο	Ν	Ι	Α	Ζ	Ξ	Κ	Ν	Γ	Ν	Α	Γ	Ι	Δ	Η
Γ	Θ	Β	Α	Ξ	Ρ	Λ	Ο	Φ	Τ	Θ	Ρ	Ψ	Ε	Ζ
Γ	Ω	Ρ	Η	Χ	Φ	Θ	Ε	Π	Τ	Ν	Τ	Α	Κ	Τ
Α	Ρ	Σ	Η	Ν	Ω	Ζ	Σ	Ο	Ρ	Υ	Ε	Δ	Π	Τ
Ρ	Κ	Ρ	Υ	Π	Τ	Ο	Γ	Ρ	Α	Φ	Η	Σ	Η	Σ
Η	Λ	Ο	Κ	Α	Τ	Α	Γ	Ρ	Α	Φ	Η	Λ	Μ	Σ
Σ	Θ	Π	Ρ	Ω	Τ	Ο	Κ	Ο	Λ	Λ	Ο	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

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

ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

2 οριζόντια: ΠΡΩΤΟΚΟΛΛΟ Τυπικό σύνολο κανόνων για σύνδεση πελάτη προς τοποθεσία (10 γράμματα)

4 οριζόντια: ΚΡΥΠΤΟΓΡΑΦΗΣΗ Κρυπτογραφική αλλοίωση των πακέτων (13 γράμματα)

7 οριζόντια: ΠΑΡΑΓΟΝΤΕΣ Ασφάλεια σύνδεσης που απαιτεί επιπλέον διακριτικά (10 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΣΗΡΑΓΓΟΠΟΙΗΣΗ Ενθυλάκωση δεδομένων σε ασφαλή διαδρομή (13 γράμματα)

3 κάθετα: ΕΥΡΟΖΩΝΗΣ Όριο χωρητικότητας δεδομένων του δικτύου (10 γράμματα)

4 κάθετα: ΚΑΤΑΓΡΑΦΗ Συγκέντρωση των αρχείων ασφαλείας σε έναν κεντρικό συλλέκτη (9 γράμματα)

5 κάθετα: ΤΕΙΧΟΣ Κανόνες του συστήματος φιλτραρίσματος της κίνησης (τείχος προστασίας) (6 γράμματα)

6 κάθετα: ΚΑΤΑΣΤΑΣΗ Επικύρωση της υγείας της απομακρυσμένης συσκευής (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. ΕΝΟΓΑΠΤΣΑΡ — **ΠΑΡΑΓΟΝΤΕΣ**
2. ΗΚΣΑΑΤΑΣΤ — **ΚΑΤΑΣΤΑΣΗ**
3. ΕΖΗΩΥΣΣΟΝΡ — **ΕΥΡΟΣΖΩΝΗΣ**
4. ΓΣΟΡΠΓΗΟΗΙΣΗΑ — **ΣΗΡΑΓΓΟΠΟΙΗΣΗ**
5. ΛΚΟΡΤΟΟΠΛΩ — **ΠΡΩΤΟΚΟΛΛΟ**
6. ΦΑΑΑΡΚΓΗΤ — **ΚΑΤΑΓΡΑΦΗ**
7. ΦΗΡΟΚΡΑΤΗΣΥΓΠ — **ΚΡΥΠΤΟΓΡΑΦΗΣΗ**
8. ΙΣΤΟΧΕ — **ΤΕΙΧΟΣ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"Η ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΠΡΟΣΒΑΣΗ ΠΡΟΣΤΑΤΕΥΕΙ ΣΥΣΚΕΥΕΣ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Επιβολή MFA

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένας επιχειρηματικός αναλυτής προσπαθεί να συνδεθεί στην εταιρική βάση δεδομένων ενώ εργάζεται εξ αποστάσεως. Εισάγει το σωστό όνομα χρήστη και κωδικό πρόσβασης, αλλά η πύλη VPN αποκλείει την πρόσβαση και ζητά κωδικό από φυσικό διακριτικό.
- Προτεινόμενη στρατηγική και λύση: Η πύλη του εταιρικού VPN επιβάλλει αυστηρή πολιτική ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) για την ασφάλεια των απομακρυσμένων συνδέσεων.

B Μελέτη περίπτωσης 2: Συμμόρφωση στάσης ασφαλείας

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένας εργολάβος συνδέει τον προσωπικό του φορητό υπολογιστή στο απομακρυσμένο εταιρικό δίκτυο. Ο πελάτης VPN διακόπτει αμέσως τη σύνδεση, ειδοποιώντας τον χρήστη ότι οι ορισμοί antivirus είναι παρωχημένοι.
- Προτεινόμενη στρατηγική και λύση: Η πύλη απομακρυσμένης πρόσβασης πραγματοποίησε έλεγχο κατάστασης του τερματικού και απέκλεισε τη συσκευή λόγω παρωχημένων ρυθμίσεων ασφαλείας.