Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

Ασφάλεια και κρυπτογράφηση δημόσιου Wi-Fi

Επιθέσεις man-in-the-middle, κακόβουλα σημεία πρόσβασης, υποκλοπή πακέτων, τούνελ VPN και κρυπτογράφηση HTTPS.

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ: ΑΣΦΑΛΕΙΑ ΔΗΜΟΣΙΟΥ WI-FI

ΑΣΦΑΛΙΣΜΕΝΟ
ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΕΔΟΜΕΝΩΝ
Πρότυπο AES 256 bit

ΣΥΜΦΩΝΟ
ΠΑΓΚΟΣΜΙΑ ΠΡΟΤΥΠΑ
Πλαίσια GDPR και CCPA

ZERO-TRUST
ΠΟΛΙΤΙΚΗ ΠΡΟΣΒΑΣΗΣ
Έλεγχος ταυτότητας πολλαπλών παραγόντων

Καλώς ήρθες! Αυτό το φυλλάδιο δραστηριοτήτων σε καθοδηγεί στην ασφάλεια του δημόσιου Wi-Fi. Θα εξερευνήσεις μη κρυπτογραφημένα δίκτυα, επιθέσεις man-in-the-middle (MitM), κακόβουλα σημεία πρόσβασης, υποκλοπή πακέτων, σήραγγες VPN και ασφάλεια μετάδοσης HTTPS.

ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ ΤΟΥ ΦΥΛΛΟΥ ΕΡΓΑΣΙΑΣ

- [ ] **Μέρη 1-4: Κατάκτησε την κυβερνοασφάλεια και την πρόληψη απειλών.**
- [ ] **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 την κυβερνοασφάλεια

URL: https://www.vpn.com/el/kiberasfaleia/asfaleia-dimosion-diktyon-wifi/

Η πορεία μάθησής σου: ασφάλεια δημόσιου Wi-Fi

- Αναγνώρισε τους συνήθεις κινδύνους του δημόσιου Wi-Fi, όπως η υποκλοπή πακέτων (packet sniffing) και τα παράνομα σημεία πρόσβασης.
- Εφάρμοσε σήραγγες κρυπτογράφησης VPN για την ασφάλεια των δεδομένων κατά τη μεταφορά.
- Επέβαλε HTTPS και ασφαλείς ρυθμίσεις προγράμματος περιήγησης για απομακρυσμένους εργαζόμενους.

ΟΔΗΓΙΕΣ ΓΙΑ ΤΟΝ ΟΔΗΓΟ ΑΣΦΑΛΕΙΑΣ ΔΗΜΟΣΙΟΥ WI-FI

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 ασφάλεια απομακρυσμένης πρόσβασης. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΑΣΦΑΛΕΙΑ ΔΗΜΟΣΙΟΥ WI-FI ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΚΑΤΑ ΤΗ ΜΕΤΑΦΟΡΑ (ΕΙΣΑΓΩΓΗ)

Τα μη κρυπτογραφημένα δημόσια σημεία πρόσβασης Wi-Fi αφήνουν την κίνηση δικτύου εκτεθειμένη σε packet sniffing και πλαστογράφηση Evil Twin. Η δρομολόγηση της κίνησης μέσω ασφαλών κρυπτογραφημένων σηράγγων VPN και η επιβολή κανόνων HSTS μόνο για HTTPS προστατεύουν τις συνεδρίες από την τοπική υποκλοπή δικτύου.

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **1. Τι είναι μια επίθεση Man-in-the-Middle (MitM);**
   - A. Υποκλοπή και αλλοίωση των επικοινωνιών μεταξύ δύο μερών σε κοινόχρηστο δίκτυο
   - B. Μια τεχνική εξαγωγής δεδομένων από βάσεις δεδομένων που στοχεύει εγγραφές χρηστών
   - C. Υπερφόρτωση διακομιστών ιστού με αιτήματα δικτυακής κίνησης
   - D. Διαγραφή τόμων αποθήκευσης του τοπικού σκληρού δίσκου

2. **2. Τι είναι ένα κακόβουλο σημείο πρόσβασης (Evil Twin);**
   - A. Ένα κακόβουλο σημείο πρόσβασης Wi-Fi ρυθμισμένο με το ίδιο SSID με ένα νόμιμο δίκτυο
   - B. Ένα διαχειριστικό εργαλείο που χρησιμοποιείται για την παρακολούθηση των αντιγράφων ασφαλείας βάσεων δεδομένων
   - C. Μια ασφαλής διαμόρφωση πύλης VPN
   - D. Μια εγγραφή DNS που αντιστοιχίζει εξουσιοδοτημένους διακομιστές αλληλογραφίας

3. **3. Πώς προστατεύει ένα VPN την κίνηση σε δημόσιο Wi-Fi;**
   - A. Τυλίγει όλα τα πακέτα δικτύου σε κρυπτογραφημένη σήραγγα, καθιστώντας τα μη αναγνώσιμα για τους sniffers
   - B. Αποκλείει αυτόματα όλα τα εισερχόμενα αιτήματα σύνδεσης
   - C. Αλλάζει τη διεύθυνση MAC της φυσικής κάρτας δικτύου
   - D. Διαγράφει τα αποθηκευμένα cookies στο πρόγραμμα περιήγησης

4. **4. Τι είναι η υποκλοπή πακέτων (packet sniffing);**
   - A. Χρήση εργαλείων υλικού ή λογισμικού για την καταγραφή πακέτων δικτύου
   - B. Σάρωση τοπικών καταλόγων για διπλότυπα αρχεία
   - C. Περιορισμός των δικαιωμάτων ανάγνωσης της βάσης δεδομένων με βάση τους ρόλους των χρηστών
   - D. Κρυπτογράφηση μονάδων αποθήκευσης με κλειδιά AES-256

5. **5. Ποιος είναι ο ρόλος του HTTPS;**
   - A. Κρυπτογράφηση της κίνησης της συνεδρίας μεταξύ του προγράμματος περιήγησης και του διακομιστή ιστού
   - B. Φιλτράρισμα εισερχόμενων μηνυμάτων email στην πύλη
   - C. Συμπίεση εικόνων για ταχύτερη φόρτωση σελίδων
   - D. Διαχείριση δομών αρχείων σε αποθήκευση συνδεδεμένη στο δίκτυο

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Οι συνδεδεμένοι χρήστες μπορούν εύκολα να καταγράψουν δεδομένα σε απλό κείμενο σε ανοιχτά δημόσια δίκτυα Wi-Fi.

○ Σωστό ○ Λάθος

7 Ερώτηση 7

7. Τα παράνομα σημεία πρόσβασης (Evil Twins) είναι πάντα εξουσιοδοτημένα από τους διαχειριστές δικτύου.

○ Σωστό ○ Λάθος

8 Ερώτηση 8

8. Ένα VPN είναι αναποτελεσματικό στην προστασία της κίνησης από την υποκλοπή πακέτων (packet sniffing) σε δημόσια δίκτυα.

○ Σωστό ○ Λάθος

9 Ερώτηση 9

9. Το HTTPS κρυπτογραφεί μόνο τη διαδρομή του URL, αφήνοντας το φορτίο των πακέτων σε απλό κείμενο.

○ Σωστό ○ Λάθος

10 Ερώτηση 10

10. Τα σημεία πρόσβασης Wi-Fi που χρησιμοποιούν ασφάλεια WPA3 προσφέρουν ισχυρότερη προστασία από τα ανοιχτά δίκτυα χωρίς κωδικό πρόσβασης.

○ 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 καταγραφή ιδιωτικών κωδικών σε δημόσιο Wi-Fi είναι η _____ της επικοινωνίας.

2. Η ανάλυση ακατέργαστων πακέτων σε τοπικό δίκτυο χρησιμοποιεί την _____ πακέτων.

3. Ένα παράνομο hotspot που μιμείται το Wi-Fi ενός ξενοδοχείου είναι ένας κακόβουλος _____ .

4. Η ασφάλιση της μετάδοσης κίνησης ιστού απαιτεί κρυπτογράφηση με _____ .

5. Η κρυπτογράφηση όλων των εξερχόμενων δεδομένων δικτύου χρησιμοποιεί έναν πελάτη _____ .

6. Μια κρυπτογραφημένη διαδρομή επικοινωνίας μέσα από δημόσια δίκτυα είναι μια _____ .

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΑΝΙΧΝΕΥΣΗ ΔΙΔΥΜΟΣ ΙΔΙΩΤΙΚΟ ΣΗΡΑΓΓΑ VPN ΤΕΙΧΟΣ ΥΠΟΚΛΟΠΗ HTTPS

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών ασφάλειας

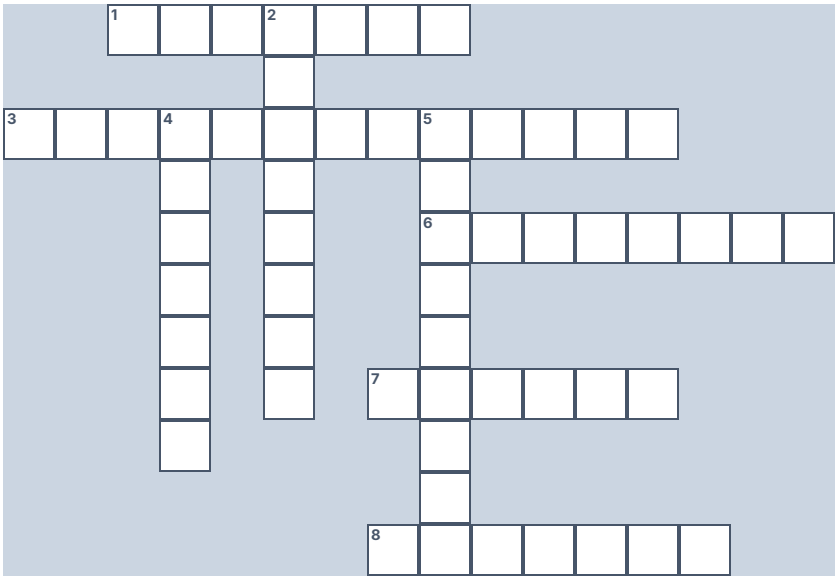
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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

☐	1. ΥΠΟΚΛΟΠΗ	A	Σύγχρονο πρότυπο ασφάλειας Wi-Fi.
☐	2. ΥΠΟΚΛΟΠΗ ΠΑΚΕΤΩΝ	B	Ασφαλής διαδρομή δεδομένων κατά τη μεταφορά.
☐	3. ΚΑΚΟΒΟΥΛΟΣ ΔΙΔΥΜΟΣ	C	Φιλτράρισμα εισερχόμενης κίνησης.
☐	4. HTTPS	D	Παράνομο hotspot που μιμείται Wi-Fi.
☐	5. VPN	E	Ανάγνωση της κίνησης κατά τη μεταφορά.
☐	6. ΤΟΥΝΕΛ	F	Καταγραφή πακέτων δεδομένων δικτύου.
☐	7. WPA3	G	Κρυπτογραφημένο εικονικό ιδιωτικό δίκτυο.
☐	8. ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ	H	Ασφαλής μετάδοση στον ιστό.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

1. Παράνομο hotspot που μιμείται ένα Wi-Fi (evil twin) (7)

3. Κωδικοποίηση της ιστοσελίδας ώστε η μετάδοση να είναι ασφαλής, όπως στις διευθύνσεις https (13)

6. Κρυπτογραφημένο εικονικό ιδιωτικό δίκτυο (VPN) (8)

7. Φιλτράρισμα της εισερχόμενης κίνησης (τείχος προστασίας) (6)

8. Ασφαλής διαδρομή δεδομένων κατά τη μετάδοση (7)

ΚΑΘΕΤΑ

2. Ανάγνωση της κίνησης κατά τη μετάδοση (8)

4. Σύγχρονο πρότυπο ασφάλειας Wi-Fi (WPA3) (7)

5. Καταγραφή πακέτων δεδομένων δικτύου (sniffing) (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

1 οριζόντια: Παράνομο hotspot που μιμείται ένα Wi-Fi (evil twin) (7 γράμματα):

3 οριζόντια: Κωδικοποίηση της ιστοσελίδας ώστε η μετάδοση να είναι ασφαλής, όπως στις διευθύνσεις https (13 γράμματα):

6 οριζόντια: Κρυπτογραφημένο εικονικό ιδιωτικό δίκτυο (VPN) (8 γράμματα):

7 οριζόντια: Φιλτράρισμα της εισερχόμενης κίνησης (τείχος προστασίας) (6 γράμματα):

8 οριζόντια: Ασφαλής διαδρομή δεδομένων κατά τη μετάδοση (7 γράμματα):

ΚΑΘΕΤΑ

2 κάθετα: Ανάγνωση της κίνησης κατά τη μετάδοση (8 γράμματα):

4 κάθετα: Σύγχρονο πρότυπο ασφάλειας Wi-Fi (WPA3) (7 γράμματα):

5 κάθετα: Καταγραφή πακέτων δεδομένων δικτύου (sniffing) (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.

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

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΥΠΟΚΛΟΠΗ ΑΝΙΧΝΕΥΣΗ ΔΙΔΥΜΟΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΙΔΙΩΤΙΚΟ ΣΗΡΑΓΓΑ
ΠΡΟΤΥΠΟ 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. ΥΠΟΚΛΟΠΗ

B. ΑΝΙΧΝΕΥΣΗ

C. ΔΙΔΥΜΟΣ

D. ΚΡΥΠΤΟΓΡΑΦΗΣΗ

E. ΙΔΙΩΤΙΚΟ

F. ΣΗΡΑΓΓΑ

G. ΠΡΟΤΥΠΟ

H. ΤΕΙΧΟΣ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

_____ 1. Σύγχρονο πρότυπο ασφάλειας Wi-Fi (WPA3).

_____ 2. Παράνομο hotspot που μιμείται ένα Wi-Fi (evil twin).

_____ 3. Καταγραφή πακέτων δεδομένων δικτύου (sniffing).

_____ 4. Ασφαλής διαδρομή δεδομένων κατά τη μετάδοση.

_____ 5. Φιλτράρισμα της εισερχόμενης κίνησης (τείχος προστασίας).

_____ 6. Ανάγνωση της κίνησης κατά τη μετάδοση.

_____ 7. Κρυπτογραφημένο εικονικό ιδιωτικό δίκτυο (VPN).

_____ 8. Κωδικοποίηση της ιστοσελίδας ώστε η μετάδοση να είναι ασφαλής, όπως στις διευθύνσεις https.

Σημείο ελέγχου 7: Πρόκληση ανακατεμένων λέξεων

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

1. **ΠΚΛΥΟΠΗΟ** _____

2. **ΔΔΣΟΜΥΙ** _____

3. **ΩΔΙΤΙΟΚΙ** _____

4. **ΟΡΥΤΠΠΟ** _____

5. **ΥΝΝΗΕΧΑΣΙ** _____

6. **ΤΦΓΟΗΥΣΑΚΡΡΗΠ** _____

7. **ΣΓΓΑΗΑΡ** _____

8. **ΙΣΤΟΧΕ** _____

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	**Λόγοι για να ενημερώνεις το λογισμικό**			
2	**Συσκευές που συνδέονται αυτόματα σε Wi-Fi**			
3	**Πληροφορίες που δεν πρέπει ποτέ να μοιράζεσαι**			
4	**Ασφαλείς συνήθειες που μπορείς να ξεκινήσεις σήμερα**			
5	**Τρόποι να μένεις ασφαλής σε ένα καφέ**			
6	**Συσκευές που μπορούν να παραβιαστούν**			
7	**Πράγματα που μπορεί να δει ένας χάκερ σε ανοιχτό Wi-Fi**			
8	**Ενδείξεις ενός ψεύτικου δικτύου Wi-Fi**			
9	**Εναλλακτικές λύσεις αντί για το δημόσιο Wi-Fi**			
10	**Προειδοποιητικά σημάδια σε ένα email**			
11	**Πράγματα που δεν κάνεις στο δημόσιο Wi-Fi**			
12	**Μέρη με δωρεάν Wi-Fi**			
13	**Τρόποι να προστατεύσεις τους λογαριασμούς σου**			
14	**Ενδείξεις ότι ένας υπολογιστής έχει μολυνθεί**			
15	**Ονόματα Wi-Fi που φαίνονται ύποπτα**			

Σημείο ελέγχου 8: Μελέτες περίπτωσης κυβερνοασφάλειας

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

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΠΕΡΙΟΡΙΣΜΟΣ ΥΠΟΚΛΟΠΗΣ ΠΑΚΕΤΩΝ ΣΕ ΔΗΜΟΣΙΟ WI-FI



Σενάριο: Ένα απομακρυσμένο στέλεχος πωλήσεων συνδεδεμένο σε δημόσιο δίκτυο Wi-Fi αεροδρομίου παρατηρεί ότι αρκετά ευαίσθητα επιχειρηματικά email διέρρευσαν λίγο μετά την αποστολή τους ως απλό κείμενο.

Ερώτηση συζήτησης: Ανάλυσε τους κινδύνους των δημόσιων δικτύων και περίγραψε συνοπτικά μια λύση κρυπτογράφησης της κίνησης.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΑΜΥΝΑ ΑΠΕΝΑΝΤΙ ΣΕ ΚΑΚΟΒΟΥΛΟ HOTSPOT EVIL TWIN



Σενάριο: Επιτιθέμενοι στήνουν ένα πλαστό ασύρματο σημείο πρόσβασης με το όνομα «CoffeeShop_Guest» που μιμείται ένα νόμιμο hotspot καφέ και συλλαμβάνει την κίνηση δικτύου από αναποφάσιστους επισκέπτες.

Ερώτηση συζήτησης: Περίγραψε αναλυτικά τα βήματα επαλήθευσης για τον εντοπισμό και τον αποκλεισμό πλαστών σημείων πρόσβασης.

Σημείο ελέγχου 9: Αποκρυπτογράφησε τον κώδικα

Ένας επαγγελματίας κυβερνοασφάλειας προστατεύει τα περιουσιακά στοιχεία του δικτύου από διαδικτυακούς φορείς απειλών. 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

10	17	20	16	19	15	3	17	1	21	7	18	5		19	7	13

10	9	13	7	18	7		12	5		18	7	17	1	3	3	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 την κυβερνοασφάλεια – βασικό επίπεδο (Μέρος Α)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για τον μετριασμό των διαδικτυακών απειλών.

Q1: Γιατί το δημόσιο Wi-Fi είναι ανασφαλές;

Το ανοιχτό δημόσιο Wi-Fi δεν κρυπτογραφεί την κίνηση στον αέρα, οπότε όσοι βρίσκονται κοντά μπορούν να καταγράψουν τυχόν απροστάτευτα δεδομένα. [2]

Q2: Τι είναι η υποκλοπή πακέτων (packet sniffing);

Ένας packet sniffer καταγράφει ακατέργαστα δεδομένα που ρέουν μέσω μιας διεπαφής δικτύου, εκθέτοντας κωδικούς πρόσβασης σε απλό κείμενο και λεπτομέρειες της κίνησης.

Q3: Τι είναι το Evil Twin;

Ένα κακόβουλο σημείο πρόσβασης που στήνουν χάκερ και μιμείται το όνομα και τις ρυθμίσεις ενός αξιόπιστου τοπικού σημείου πρόσβασης Wi-Fi.

Q4: Πώς με προστατεύει ένα VPN;

Δρομολογεί την κίνησή σου μέσω κρυπτογραφημένης σήραγγας, κρύβοντας τη δραστηριότητα περιήγησής σου από τους υποκλοπείς του τοπικού δικτύου.

Q5: Με προστατεύει το HTTPS σε δημόσιο Wi-Fi;

Ναι, κρυπτογραφεί τα δεδομένα που ανταλλάσσονται ανάμεσα στο πρόγραμμα περιήγησης και τον ιστότοπο, και ένα VPN προσθέτει ένα ακόμη επίπεδο προστασίας.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την κυβερνοασφάλεια – βασικό επίπεδο (Μέρος Β)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για τον μετριασμό των διαδικτυακών απειλών.

Q6: Τι είναι το WPA3;

Το σύγχρονο πρότυπο Wi-Fi Protected Access, που προσφέρει ισχυρότερη κρυπτογράφηση και προστασία από επιθέσεις λεξικού εκτός σύνδεσης. [1]

Q7: Μπορεί το δημόσιο Wi-Fi να διανείμει κακόβουλο λογισμικό;

Ναι, οι επιτιθέμενοι μπορούν να υποκλέψουν την κίνηση και να εισάγουν κακόβουλα αιτήματα λήψης (drive-by downloads) στη συνεδρία του προγράμματος περιήγησής σου.

Q8: Ποιος είναι ο κίνδυνος της κοινής χρήσης αρχείων;

Αν η κοινή χρήση αρχείων είναι ενεργοποιημένη, άλλοι χρήστες στο δημόσιο δίκτυο μπορούν να διαβάσουν ή να τροποποιήσουν τον τοπικό σου φάκελο.

Q9: Τι είναι μια πύλη εξουσιοδότησης δικτύου (captive portal);

Η σελίδα σύνδεσης που χρησιμοποιούν τα δίκτυα ξενοδοχείων ή καφέ για να παραχωρήσουν πρόσβαση στο διαδίκτυο και η οποία μπορεί μερικές φορές να πλαστογραφηθεί από επιτιθέμενους.

Q10: Πρέπει να απενεργοποιώ το Wi-Fi όταν δεν το χρησιμοποιώ;

Ναι, η απενεργοποίηση του Wi-Fi εμποδίζει τη συσκευή σου να συνδέεται αυτόματα σε μη αξιόπιστα δίκτυα.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την ασφάλεια – προχωρημένο επίπεδο (Μέρος C)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πλαισίων ασφάλειας, της ανάλυσης κακόβουλου λογισμικού και της συμμόρφωσης δεδομένων.

Q1: Πώς εκμεταλλεύεται το DNS μια επίθεση Man-in-the-Middle;

Χρησιμοποιώντας πλαστογράφηση DNS (DNS spoofing) σε παράνομο δρομολογητή για να κατευθύνει τα προγράμματα περιήγησης-στόχους σε ψεύτικες σελίδες ηλεκτρονικού ψαρέματος (phishing) αντί για τα ονόματα τομέα-στόχους.

Q2: Τι είναι η υφαρπαγή συνεδρίας (session hijacking);

Ένας επιτιθέμενος που υποκλέπτει ένα μη κρυπτογραφημένο cookie συνεδρίας σε δημόσιο Wi-Fi και το εισάγει για να παρακάμψει τις συνδέσεις με διαπιστευτήρια.

Q3: Τι είναι το SSL stripping;

Μια επίθεση MitM όπου ο επιτιθέμενος υποβαθμίζει ένα ασφαλές αίτημα HTTPS του χρήστη σε μη κρυπτογραφημένο HTTP, καταγράφοντας τα στοιχεία σύνδεσης σε απλό κείμενο.

Q4: Πώς προστατεύει το HSTS από το SSL stripping;

Το HTTP Strict Transport Security υποχρεώνει τα προγράμματα περιήγησης να συνδέονται μόνο μέσω HTTPS και να αρνούνται τις μη κρυπτογραφημένες εναλλακτικές HTTP. [3]

Q5: Τι είναι ένα VPN με split tunneling;

Μια διαμόρφωση που δρομολογεί μόνο την εταιρική κίνηση μέσω του VPN ενώ στέλνει τα δημόσια δεδομένα διαδικτύου απευθείας, κάτι που μπορεί να ενέχει κίνδυνο έκθεσης λόγω διαρροής.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την ασφάλεια – προχωρημένο επίπεδο (Μέρος D)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πλαισίων ασφάλειας, της ανάλυσης κακόβουλου λογισμικού και της συμμόρφωσης δεδομένων.

Q6: Γιατί το WPA2 είναι ευάλωτο στην επίθεση KRACK;

Η Key Reinstallation Attack εκμεταλλεύεται την τετραπλή χειραψία του WPA2 για να αποκρυπτογραφήσει πακέτα χωρίς τον κωδικό πρόσβασης του Wi-Fi.

Q7: Τι είναι η απομόνωση πελατών (client isolation);

Μια ρύθμιση ασφαλείας δρομολογητή που εμποδίζει τις συνδεδεμένες συσκευές Wi-Fi να επικοινωνούν απευθείας μεταξύ τους, αποκλείοντας την τοπική υποκλοπή.

Q8: Πώς χρησιμοποιούν οι επιτιθέμενοι πλαστούς διακομιστές DNS;

Ρυθμίζουν κακόβουλους δρομολογητές να αναθέτουν ψεύτικους διακομιστές DNS στους πελάτες, επιτρέποντάς τους να υποκλέπτουν και να τροποποιούν όλες τις αναζητήσεις ιστού.

Q9: Μπορεί ένα VPN να κρύψει την τοπική μου διεύθυνση MAC;

Όχι. Οι διευθύνσεις MAC είναι τοπικά αναγνωριστικά επιπέδου 2· χρησιμοποίησε αντί γι' αυτό την ενσωματωμένη ρύθμιση τυχαιοποίησης MAC (ιδιωτική διεύθυνση) της συσκευής σου.

Q10: Τι είναι μια επίθεση πλαστοπροσωπίας captive portal;

Ένας επιτιθέμενος που φιλοξενεί μια ψεύτικη πύλη ταυτοποίησης σε ένα κακόβουλο σημείο πρόσβασης για να κλέψει διαπιστευτήρια με το πρόσχημα δωρεάν πρόσβασης Wi-Fi.

Μέρος 11: 10 πραγματικά στοιχεία και διαπιστώσεις για την κυβερνοασφάλεια

Εξέτασε πραγματικά στοιχεία για τις παραβιάσεις ασφαλείας, τους μηχανισμούς άμυνας και τα πρότυπα συμμόρφωσης.

1. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι απομακρυσμένοι εργαζόμενοι συχνά χρησιμοποιούν Wi-Fi σε καφέ, ξενοδοχεία και αεροδρόμια, όπου δεν μπορούν να ελέγξουν την ασφάλεια του δικτύου.

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Ένα κακόβουλο σημείο πρόσβασης Evil Twin μπορεί να αντιγράψει το ακριβές όνομα και τη διεύθυνση MAC ενός αξιόπιστου δικτύου, μπερδεύοντας τις συσκευές.

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Λογισμικό υποκλοπής πακέτων όπως το Wireshark είναι δωρεάν και μπορεί να εμφανίσει μη κρυπτογραφημένους κωδικούς HTTP σε απλό κείμενο.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η ασφάλεια WPA3 χρησιμοποιεί τη διαδικασία Simultaneous Authentication of Equals (SAE) για προστασία από τοπικές επιθέσεις ωμής βίας.

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι επιθέσεις SSL stripping παρακάμπτουν τις βασικές προστασίες HTTPS υποκλέπτοντας τις αρχικές ανακατευθύνσεις HTTP στην πύλη.

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι κεφαλίδες απόκρισης HTTP Strict Transport Security (HSTS) εμποδίζουν τα προγράμματα περιήγησης να επιστρέφουν σε μη κρυπτογραφημένες συνδέσεις HTTP. [3]

7. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η απενεργοποίηση του «Auto-Connect» εμποδίζει τα smartphone να συνδέονται σε πλαστά δίκτυα που μιμούνται άλλα σε δημόσιους χώρους.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι επιχειρησιακές διαμορφώσεις VPN «always-on» υποχρεώνουν όλη την κίνηση δικτύου των απομακρυσμένων εργαζομένων να περνά από εταιρικά τείχη προστασίας.

9. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Τα παράνομα σημεία πρόσβασης μπορούν να δίνουν πλαστές απαντήσεις DNS, ανακατευθύνοντας τους στοχευμένους τομείς σε διακομιστές ηλεκτρονικού ψαρέματος.

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Χωρίς VPN, άλλοι χρήστες σε ένα ανοιχτό hotspot μπορούν να δουν ποιους ιστότοπους και διακομιστές επικοινωνεί η συσκευή σου.

Τεχνικές αναφορές και πηγές

Ο οδηγός μελέτης και τα διαδραστικά παζλ έχουν συνταχθεί από παγκόσμια πρότυπα NIST, OWASP και συμμόρφωσης με την ιδιωτικότητα των δεδομένων.

ΑΚΑΔΗΜΑΪΚΕΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 Ερώτηση 1

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι είναι μια επίθεση Man-in-the-Middle (MitM); → Υποκλοπή και αλλοίωση των επικοινωνιών μεταξύ δύο μερών σε κοινόχρηστο δίκτυο

2 Ερώτηση 2

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι είναι ένα κακόβουλο σημείο πρόσβασης (Evil Twin); → Ένα κακόβουλο σημείο πρόσβασης Wi-Fi ρυθμισμένο με το ίδιο SSID με ένα νόμιμο δίκτυο

3 Ερώτηση 3

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Πώς προστατεύει ένα VPN την κίνηση σε δημόσιο Wi-Fi; → Τυλίγει όλα τα πακέτα δικτύου σε κρυπτογραφημένη σήραγγα, καθιστώντας τα μη αναγνώσιμα για τους sniffers

4 Ερώτηση 4

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι είναι η υποκλοπή πακέτων (packet sniffing); → Χρήση εργαλείων υλικού ή λογισμικού για την καταγραφή πακέτων δικτύου

5 Ερώτηση 5

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ποιος είναι ο ρόλος του HTTPS; → Κρυπτογράφηση της κίνησης της συνεδρίας μεταξύ του προγράμματος περιήγησης και του διακομιστή ιστού

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 **Ερώτηση 6** — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι συνδεδεμένοι χρήστες μπορούν εύκολα να καταγράψουν δεδομένα σε απλό κείμενο σε ανοιχτά δημόσια δίκτυα Wi-Fi.

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

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: ένα Evil Twin είναι μη εξουσιοδοτημένο hotspot που στήνει ένας επιτιθέμενος για να μιμηθεί ένα πραγματικό.

8 **Ερώτηση 8** — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: ένα VPN κρυπτογραφεί την κίνηση σε τούνελ, οπότε οι τοπικοί sniffers δεν μπορούν να τη διαβάσουν.

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

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: το HTTPS κρυπτογραφεί ολόκληρη την ανταλλαγή HTTP, συμπεριλαμβανομένης της διαδρομής του URL και του περιεχομένου της σελίδας.

10 **Ερώτηση 10** — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα σημεία πρόσβασης Wi-Fi που χρησιμοποιούν ασφάλεια WPA3 προσφέρουν ισχυρότερη προστασία από τα ανοιχτά δίκτυα χωρίς κωδικό πρόσβασης.

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

E 1. ΥΠΟΚΛΟΠΗ	F 2. ΥΠΟΚΛΟΠΗ ΠΑΚΕΤΩΝ	D 3. ΚΑΚΟΒΟΥΛΟΣ ΔΙΔΥΜΟΣ	H 4. HTTPS
G 5. VPN	B 6. ΤΟΥΝΕΛ	A 7. WPA3	C 8. ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΥΠΟΚΛΟΠΗ	2 ΑΝΙΧΝΕΥΣΗ	3 ΔΙΔΥΜΟΣ	4 HTTPS
5 VPN	6 ΣΗΡΑΓΓΑ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 G – ΠΡΟΤΥΠΟ	2 C – ΔΙΔΥΜΟΣ	3 B – ΑΝΙΧΝΕΥΣΗ	4 F – ΣΗΡΑΓΓΑ
5 H – ΤΕΙΧΟΣ	6 A – ΥΠΟΚΛΟΠΗ	7 E – ΙΔΙΩΤΙΚΟ	8 D – ΚΡΥΠΤΟΓΡΑΦΗΣΗ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους ΥΠΟΚΛΟΠΗ, ΥΠΟΚΛΟΠΗ ΠΑΚΕΤΩΝ και ΚΑΚΟΒΟΥΛΟΣ ΔΙΔΥΜΟΣ 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

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

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ

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

ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

1 οριζόντια: ΔΙΔΥΜΟΣ Παράνομο hotspot που μιμείται ένα Wi-Fi (evil twin) (7 γράμματα)

3 οριζόντια: ΚΡΥΠΤΟΓΡΑΦΗΣΗ Κωδικοποίηση της ιστοσελίδας ώστε η μετάδοση να είναι ασφαλής, όπως στις διευθύνσεις https (13 γράμματα)

6 οριζόντια: ΙΔΙΩΤΙΚΟ Κρυπτογραφημένο εικονικό ιδιωτικό δίκτυο (VPN) (8 γράμματα)

7 οριζόντια: ΤΕΙΧΟΣ Φιλτράρισμα της εισερχόμενης κίνησης (τείχος προστασίας) (6 γράμματα)

8 οριζόντια: ΣΗΡΑΓΓΑ Ασφαλής διαδρομή δεδομένων κατά τη μετάδοση (7 γράμματα)

ΚΑΘΕΤΑ

2 κάθετα: ΥΠΟΚΛΟΠΗ Ανάγνωση της κίνησης κατά τη μετάδοση (8 γράμματα)

4 κάθετα: ΠΡΟΤΥΠΟ Σύγχρονο πρότυπο ασφάλειας Wi-Fi (WPA3) (7 γράμματα)

5 κάθετα: ΑΝΙΧΝΕΥΣΗ Καταγραφή πακέτων δεδομένων δικτύου (sniffing) (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. ΠΚΛΥΟΠΗΟ — **ΥΠΟΚΛΟΠΗ**
2. ΔΔΣΟΜΥΙ — **ΔΙΔΥΜΟΣ**
3. ΩΔΙΤΙΟΚΙ — **ΙΔΙΩΤΙΚΟ**
4. ΟΡΥΤΠΠΟ — **ΠΡΟΤΥΠΟ**
5. ΥΝΝΗΕΧΑΣΙ — **ΑΝΙΧΝΕΥΣΗ**
6. ΤΦΓΟΗΥΣΑΚΡΡΗΠ — **ΚΡΥΠΤΟΓΡΑΦΗΣΗ**
7. ΣΓΓΑΗΑΡ — **ΣΗΡΑΓΓΑ**
8. ΙΣΤΟΧΕ — **ΤΕΙΧΟΣ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΚΡΥΠΤΟΓΡΑΦΗΣΕ ΤΗΝ ΚΙΝΗΣΗ ΜΕ ΣΗΡΑΓΓΑ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Περιορισμός υποκλοπής πακέτων σε δημόσιο Wi-Fi

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένα απομακρυσμένο στέλεχος πωλήσεων συνδεδεμένο σε δημόσιο δίκτυο Wi-Fi αεροδρομίου παρατηρεί ότι αρκετά ευαίσθητα επιχειρηματικά email διέρρευσαν λίγο μετά την αποστολή τους σε απλό κείμενο.
- Προτεινόμενη στρατηγική και λύση: Επίβαλε τη χρήση εταιρικού πελάτη VPN σε όλους τους απομακρυσμένους σταθμούς εργασίας. Επίβαλε επεκτάσεις προγράμματος περιήγησης μόνο HTTPS και απέκλεισε μη κρυπτογραφημένα πρωτόκολλα (όπως HTTP και FTP) στο τείχος προστασίας του πελάτη.

B Μελέτη περίπτωσης 2: Άμυνα απέναντι σε κακόβουλο hotspot evil twin

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Επιτιθέμενοι εγκαθιστούν ένα πλαστό σημείο πρόσβασης ασύρματου δικτύου με το όνομα 'CoffeeShop_Guest', που μιμείται ένα νόμιμο hotspot καφετέριας και καταγράφει την κίνηση δικτύου των ανυποψίαστων επισκεπτών.
- Προτεινόμενη στρατηγική και λύση: Έλεγξε τις διευθύνσεις MAC BSSID των σημείων πρόσβασης για να επαληθεύσεις την αυθεντικότητα του δικτύου. Επέβαλε επικύρωση της κατάστασης του πελάτη (client posture) για να αποκλειστεί η σύνδεση σε ανοιχτά δίκτυα και απαίτησε σημεία πρόσβασης κινητής για ευαίσθητη εργασία.