Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

Σκοτεινός ιστός και βαθύς ιστός: ασφάλεια και Διαφορές

Ευρετηρίαση από μηχανές αναζήτησης, βάσεις δεδομένων του deep web, δρομολόγηση Tor onion, ανωνυμία δικτύου και κίνδυνοι

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ: ΣΚΟΤΕΙΝΟΣ ΙΣΤΟΣ ΕΝΑΝΤΙ ΒΑΘΕΟΣ ΙΣΤΟΥ

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 στις διαφορές μεταξύ Deep Web και Dark Web. Θα εξερευνήσεις μη ευρετηριασμένες βάσεις δεδομένων, δρομολόγηση Onion του προγράμματος περιήγησης Tor, κρυπτογραφικούς τομείς .onion και κινδύνους ασφάλειας της ανωνυμίας.

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/dark-web-vs-deep-web/

Η πορεία μάθησής σου: στρατηγική για το βαθύ και σκοτεινό διαδίκτυο

- Αντιπαράθεσε τον βαθύ ιστό (μη ευρετηριασμένες βάσεις δεδομένων) με τον σκοτεινό ιστό (υπηρεσίες onion).
- Κατανόησε πώς η δρομολόγηση Onion κρυπτογραφεί και αναμεταδίδει την κίνηση δικτύου.
- Αξιολόγησε τους κινδύνους ασφάλειας από την πρόσβαση σε μη επαληθευμένους ιστότοπους του δικτύου Tor.
- Ανάπτυξε ασφαλείς πολιτικές πύλης και sandboxing για την ανίχνευση πληροφοριών απειλών.
- Ανάλυσε τη μορφή κρυπτογραφικής διεύθυνσης των domain υπηρεσιών onion.

ΟΔΗΓΙΕΣ ΓΙΑ ΤΟΝ ΒΑΘΥ ΚΑΙ ΤΟ ΣΚΟΤΕΙΝΟ ΔΙΑΔΙΚΤΥΟ

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 ιδιωτικότητα στο βαθύ και στο σκοτεινό διαδίκτυο. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ ΤΟΥ ΒΑΘΕΟΣ ΙΣΤΟΥ ΕΝΑΝΤΙ ΔΡΟΜΟΛΟΓΗΣΗΣ ONION ΤΟΥ ΣΚΟΤΕΙΝΟΥ ΙΣΤΟΥ (ΕΙΣΑΓΩΓΗ)

Το deep web αποτελείται από μη ευρετηριασμένες σελίδες πίσω από κωδικούς πρόσβασης και συνδέσεις, όπως ιδιωτικά email ή εταιρικές τραπεζικές πύλες. Το dark web είναι υποσύνολο του deep web που είναι σκόπιμα κρυμμένο και απαιτεί εξειδικευμένα προγράμματα περιήγησης (όπως το Tor) και δίκτυα onion για ανώνυμη πρόσβαση.

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. Τι διακρίνει το βαθύ διαδίκτυο (deep web) από το επιφανειακό διαδίκτυο (surface web);

- A. Οι σελίδες του βαθέος ιστού δεν ευρετηριάζονται από τις δημόσιες μηχανές αναζήτησης
- B. Η κίνηση στο βαθύ διαδίκτυο είναι παράνομη και παρακολουθείται από τις αρχές επιβολής του νόμου
- C. Οι ιστότοποι του βαθύ διαδικτύου απαιτούν εξειδικευμένα προγράμματα περιήγησης όπως το Tor για την πρόσβαση
- D. Οι σελίδες του βαθέος ιστού φορτώνουν πάντα ταχύτερα από τις σελίδες του επιφανειακού ιστού

2. Πώς γίνεται η πρόσβαση στο dark web;

- A. Μέσω εξειδικευμένων προγραμμάτων περιήγησης που χρησιμοποιούν δίκτυα δρομολόγησης onion
- B. Με τη ρύθμιση προσαρμοσμένων ρυθμίσεων DNS σε τυπικούς δρομολογητές
- C. Μέσω ιδιωτικών κονσολών αναζήτησης επιφανειακού ιστού μόνο με πρόσκληση
- D. Με εγκατάσταση μιας τυπικής επέκτασης προγράμματος περιήγησης για αποκλεισμό διαφημίσεων

3. Ποια δομή αποτελεί το μεγαλύτερο μέρος του βαθέος διαδικτύου (deep web);

- A. Βάσεις δεδομένων χρηστών και ιδιωτικοί λογαριασμοί προστατευμένοι με κωδικό πρόσβασης
- B. Παράνομα φόρουμ μαύρης αγοράς όπου διακινούνται παράνομα αγαθά
- C. Μη κρυπτογραφημένα πρωτόκολλα κοινής χρήσης αρχείων peer-to-peer
- D. Δημόσιες βάσεις δεδομένων προσωρινής αποθήκευσης μηχανών αναζήτησης

4. Τι κάνει η δρομολόγηση Onion στην κίνηση του δικτύου;

- A. Κρυπτογραφεί τα πακέτα και τα δρομολογεί μέσω πολλαπλών αναμεταδοτών
- B. Αυξάνει τις ταχύτητες λήψης παρακάμπτοντας τους κόμβους του ISP
- C. Αντιστοιχίζει τους σειριακούς αριθμούς υλικού της συσκευής με εγγραφές IP
- D. Διαγράφει τα cookies του προγράμματος περιήγησης μετά από κάθε κλικ

5. Ποιο επίθημα τομέα χρησιμοποιείται αποκλειστικά στα δίκτυα Tor;

- A. Η κρυπτογραφική κατάληξη ανώτατου επιπέδου .onion
- B. Η τυπική παλαιού τύπου εμπορική κατάληξη .com
- C. Η αποκεντρωμένη κατάληξη blockchain .eth του Web3
- D. Η κατάληξη τεχνολογίας χώρας .ai

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση Σωστό/Λάθος 6

6. Το deep web και το dark web αναφέρονται στο ίδιο τμήμα του δικτύου.

- ◯ Σωστό
- ◯ Λάθος

7 Ερώτηση Σωστό/Λάθος 7

7. Οι πύλες εταιρικού intranet ανήκουν στον βαθύ ιστό.

- ◯ Σωστό
- ◯ Λάθος

8 Ερώτηση Σωστό/Λάθος 8

8. Η δρομολόγηση onion αποκρυπτογραφεί πλήρως τα πακέτα δεδομένων σε κάθε ενδιάμεσο κόμβο.

- ◯ Σωστό
- ◯ Λάθος

9 Ερώτηση Σωστό/Λάθος 9

9. Η πρόσβαση στο dark web εκθέτει τις συσκευές σε υψηλούς κινδύνους κακόβουλου λογισμικού.

- ◯ Σωστό
- ◯ Λάθος

10 Ερώτηση Σωστό/Λάθος 10

10. Οι τυπικές μηχανές αναζήτησης ιστού ανιχνεύουν και ευρετηριάζουν ιστότοπους onion.

- ◯ 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 ιδιωτικές τραπεζικές πύλες βρίσκονται στο τμήμα του διαδικτύου χωρίς ευρετηρίαση, που ονομάζεται _____ .

2. Οι κρυφές υπηρεσίες που φιλοξενούν εξειδικευμένοι κόμβοι Tor ανήκουν στον: _____ .

3. Οι ιστότοποι Tor χρησιμοποιούν την κρυπτογραφική επέκταση ανώτατου επιπέδου . _____ .

4. Η κρυπτογραφημένη πολυεπίπεδη διαδρομή της κίνησης ονομάζεται _____ .

5. Οι μηχανές αναζήτησης της επιφάνειας ανιχνεύουν σελίδες που είναι δημόσια _____ .

6. Τα δίκτυα onion κρυπτογραφούν τις IP των πελατών για να διατηρούν την _____ του χρήστη.

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΑΝΑΖΗΤΗΣΙΜΕΣ ΑΝΩΝΥΜΙΑ ΒΑΘΥΣ ΙΣΤΟΣ ΒΑΣΗ ΔΕΔΟΜΕΝΩΝ ΔΡΟΜΟΛΟΓΗΣΗ
ΚΡΕΜΜΥΔΙ ΣΚΟΤΕΙΝΟΣ ΙΣΤΟΣ ONION

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών ασφάλειας

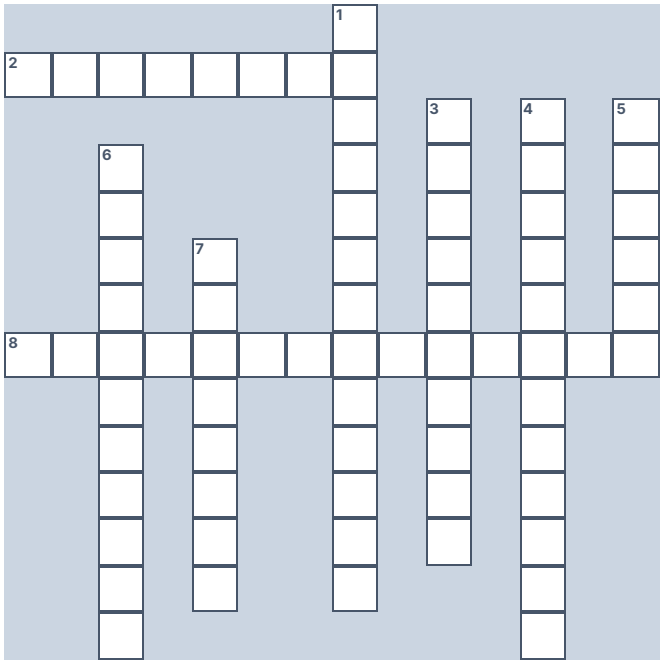
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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

☐	1. Τμήμα του βαθέος διαδικτύου (Deep Web)	A	Κρυπτογραφημένο τμήμα δικτύου προσβάσιμο μόνο μέσω ειδικών προγραμμάτων περιήγησης.
☐	2. Πύλη Dark Web	B	Κρυπτογράφηση δεδομένων σε επίπεδα και αναμετάδοσή τους μέσω τριών κόμβων.
☐	3. Επέκταση Onion	C	Ασφαλής αποθήκευση υποστήριξης (backend) που φιλοξενεί μη ευρετηριασμένες εγγραφές συστήματος.
☐	4. Δρομολόγηση Tor	D	Κρυπτογραφική κατάληξη τομέα ανώτατου επιπέδου που χρησιμοποιείται στα δίκτυα Tor.
☐	5. Ευρετηριασμένες σελίδες	E	Ο κόμβος σημείου εισόδου που χρησιμοποιείται για την πρόσβαση στο δίκτυο Tor.
☐	6. Ανωνυμία χρήστη	F	Περιεχόμενο του ορατού ιστού που έχει συγκεντρωθεί και είναι αναζητήσιμο στη Google.
☐	7. Ιδιωτική βάση δεδομένων	G	Απόκρυψη των δημόσιων διευθύνσεων IP των πελατών από τους διακομιστές.
☐	8. Πύλη εισόδου	H	Μη ευρετηριασμένο περιεχόμενο ιστού, όπως ιδιωτικές συνδέσεις, email και εγγραφές βάσεων δεδομένων.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

2. Απόκρυψη των δημόσιων διευθύνσεων IP των πελατών από τους διακομιστές (8)

8. Κρυπτογραφημένο τμήμα δικτύου που είναι προσβάσιμο μόνο μέσω ειδικών προγραμμάτων περιήγησης (14)

ΚΑΘΕΤΑ

1. Ασφαλής αποθήκευση στο παρασκήνιο που φιλοξενεί εγγραφές συστήματος χωρίς ευρετηρίαση (13)

3. Περιεχόμενο ιστού χωρίς ευρετηρίαση, όπως ιδιωτικές συνδέσεις, email και εγγραφές βάσεων δεδομένων (10)

4. Περιεχόμενο του ιστού της επιφάνειας που έχει καταγραφεί και είναι αναζητήσιμο στο Google (12)

5. Ο κόμβος εισόδου που χρησιμοποιείται για πρόσβαση στο δίκτυο Tor (6)

6. Κρυπτογράφηση των δεδομένων σε επίπεδα και αναμετάδοσή τους μέσω τριών κόμβων (11)

7. Λαχανικό με επάλληλα στρώματα, από το οποίο παίρνει το όνομά της η κατάληξη των κρυφών υπηρεσιών του Tor (8)

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: Απόκρυψη των δημόσιων διευθύνσεων IP των πελατών από τους διακομιστές (8 γράμματα):

8 οριζόντια: Κρυπτογραφημένο τμήμα δικτύου που είναι προσβάσιμο μόνο μέσω ειδικών προγραμμάτων περιήγησης (14 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Ασφαλής αποθήκευση στο παρασκήνιο που φιλοξενεί εγγραφές συστήματος χωρίς ευρετηρίαση (13 γράμματα):

3 κάθετα: Περιεχόμενο ιστού χωρίς ευρετηρίαση, όπως ιδιωτικές συνδέσεις, email και εγγραφές βάσεων δεδομένων (10 γράμματα):

4 κάθετα: Περιεχόμενο του ιστού της επιφάνειας που έχει καταγραφεί και είναι αναζητήσιμο στο Google (12 γράμματα):

5 κάθετα: Ο κόμβος εισόδου που χρησιμοποιείται για πρόσβαση στο δίκτυο Tor (6 γράμματα):

6 κάθετα: Κρυπτογράφηση των δεδομένων σε επίπεδα και αναμετάδοσή τους μέσω τριών κόμβων (11 γράμματα):

7 κάθετα: Λαχανικό με επάλληλα στρώματα, από το οποίο παίρνει το όνομά της η κατάληξη των κρυφών υπηρεσιών του Tor (8 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.

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

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΒΑΘΥΣΙΣΤΟΣ
ΣΚΟΤΕΙΝΟΣΙΣΤΟΣ
ΚΡΕΜΜΥΔΙ
ΔΡΟΜΟΛΟΓΗΣΗ
ΑΝΑΖΗΤΗΣΙΜΕΣ
ΑΝΩΝΥΜΙΑ
ΒΑΣΗΔΕΔΟΜΕΝΩΝ
ΚΟΜΒΟΣ

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. ΒΑΘΥΣΙΣΤΟΣ

B. ΣΚΟΤΕΙΝΟΣΙΣΤΟΣ

C. ΚΡΕΜΜΥΔΙ

D. ΔΡΟΜΟΛΟΓΗΣΗ

E. ΑΝΑΖΗΤΗΣΙΜΕΣ

F. ΑΝΩΝΥΜΙΑ

G. ΒΑΣΗΔΕΔΟΜΕΝΩΝ

H. ΚΟΜΒΟΣ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

_____ 1. Απόκρυψη των δημόσιων διευθύνσεων IP των πελατών από τους διακομιστές.

_____ 2. Ασφαλής αποθήκευση στο παρασκήνιο που φιλοξενεί εγγραφές συστήματος χωρίς ευρετηρίαση.

_____ 3. Κρυπτογράφηση των δεδομένων σε επίπεδα και αναμετάδοσή τους μέσω τριών κόμβων.

_____ 4. Περιεχόμενο ιστού χωρίς ευρετηρίαση, όπως ιδιωτικές συνδέσεις, email και εγγραφές βάσεων δεδομένων.

_____ 5. Κρυπτογραφημένο τμήμα δικτύου που είναι προσβάσιμο μόνο μέσω ειδικών προγραμμάτων περιήγησης.

_____ 6. Λαχανικό με επάλληλα στρώματα, από το οποίο παίρνει το όνομά της η κατάληξη των κρυφών υπηρεσιών του Tor.

_____ 7. Ο κόμβος εισόδου που χρησιμοποιείται για πρόσβαση στο δίκτυο Tor.

_____ 8. Περιεχόμενο του ιστού της επιφάνειας που έχει καταγραφεί και είναι αναζητήσιμο στο Google.

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. ΟΣΙΣΑΒΤΣΥΘ
2. ΜΚΙΡΔΥΜΕ
3. ΑΝΣΗΕΙΑΤΣΗΜΖ
4. ΕΩΜΣΟΔΝΔΝΕΒΑΗ
5. ΙΟΤΚΟΣΕΣΙΣΝΣΟΤ
6. ΟΗΛΓΣΗΔΡΟΟΜ
7. ΑΑΥΜΙΝΝΩ
8. ΜΣΚΟΒΟ

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	Λόγοι για να μένεις μακριά από το dark web			
2	Πράγματα που μια μηχανή αναζήτησης δεν μπορεί να βρει			
3	Συσκευές που μπορούν να παραβιαστούν			
4	Νόμιμοι λόγοι για να χρησιμοποιείς το Tor			
5	Λόγοι για να ενημερώνεις το λογισμικό			
6	Προειδοποιητικά σημάδια σε ένα email			
7	Πράγματα που πωλούνται παράνομα στο dark web			
8	Άνθρωποι που μπορείς να ρωτήσεις για βοήθεια στην πληροφορική			
9	Ασφαλείς συνήθειες που μπορείς να ξεκινήσεις σήμερα			
10	Πράγματα που κάνεις μετά από μια διαρροή δεδομένων			
11	Πράγματα που ανήκουν στο deep web			
12	Ιστότοποι που χρησιμοποιείς με σύνδεση			
13	Λέξεις που σχετίζονται με την ανωνυμία			
14	Πληροφορίες που δεν πρέπει ποτέ να μοιράζεσαι			
15	Πράγματα που βρίσκονται «κάτω από την επιφάνεια»			

Σημείο ελέγχου 8: Μελέτες περίπτωσης κυβερνοασφάλειας

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

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΕΝΤΟΠΙΣΜΟΣ ΔΙΑΡΡΟΗΣ ΔΕΔΟΜΕΝΩΝ



Σενάριο: Ένας εταιρικός έλεγχος ασφαλείας ανακαλύπτει ότι ευαίσθητες εγγραφές βάσεων δεδομένων πελατών διακινούνται σε μια αγορά onion. Τα δεδομένα δεν έχουν ευρετηριαστεί στο Google.

Ερώτηση συζήτησης: Εξήγησε ποια τμήματα του web εμπλέκονται και πώς έγινε αυτή η διαρροή.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΑΝΩΝΥΜΙΑ ΕΝΑΝΤΙ ΚΙΝΔΥΝΩΝ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ



Σενάριο: Ένας αναλυτής θέλει να ελέγξει τροφοδοσίες πληροφοριών απειλών σε έναν ιστότοπο Tor. Κατεβάζει το πρόγραμμα περιήγησης Tor και μπαίνει στον ιστότοπο.

Ερώτηση συζήτησης: Αξιολόγησε τα οφέλη ανωνυμίας και περίγραψε συνοπτικά τα βήματα μετριασμού κακόβουλου λογισμικού.

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

| | | |

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

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

Q1: Τι είναι το deep web;

Το deep web αποτελείται από όλες τις ιστοσελίδες που οι μηχανές αναζήτησης δεν μπορούν να ευρετηριάσουν, όπως η ηλεκτρονική τραπεζική, οι βάσεις δεδομένων email και τα περιοδικά με πληρωμένη πρόσβαση.

Q2: Τι είναι το dark web;

Το dark web είναι ένα μικρό υποσύνολο του deep web, σκόπιμα κρυμμένο και προσβάσιμο μόνο μέσω εξειδικευμένων προγραμμάτων περιήγησης που χρησιμοποιούν δίκτυα onion.

Q3: Πώς ευρετηριάζουν οι μηχανές αναζήτησης τις σελίδες;

Οι μηχανές αναζήτησης εκτελούν αυτοματοποιημένα προγράμματα (ανιχνευτές) που ακολουθούν δημόσιους συνδέσμους, ευρετηριάζοντας σελίδες που δεν αποκλείουν τη σάρωση μέσω οδηγιών robot.

Q4: Γιατί οι διαδικτυακές τραπεζικές υπηρεσίες θεωρούνται μέρος του βαθύ ιστού (deep web);

Οι τραπεζικές πύλες βρίσκονται πίσω από τείχη σύνδεσης και κωδικούς πρόσβασης, εμποδίζοντας τις δημόσιες μηχανές αναζήτησης να ευρετηριάσουν τις σελίδες των κινήσεων λογαριασμού.

Q5: Τι είναι η δρομολόγηση Onion του προγράμματος περιήγησης Tor;

Η δρομολόγηση onion είναι μια μέθοδος μετάδοσης που κρυπτογραφεί την κίνηση σε επίπεδα και την περνά μέσω πολλών αναμεταδοτών για να κρύψει τις διευθύνσεις IP των χρηστών.

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

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

Q6: Είναι παράνομη η πρόσβαση στο dark web;

Όχι. Η πρόσβαση στο dark web είναι νόμιμη στις περισσότερες χώρες, αν και απαγορεύεται η συμμετοχή σε παράνομες αγορές ή κυβερνοδραστηριότητες.

Q7: Γιατί οι ιστότοποι του dark web φορτώνουν αργά;

Η κίνηση δρομολογείται και αποκρυπτογραφείται μέσω τουλάχιστον τριών παγκόσμιων κόμβων αναμετάδοσης (εισόδου, ενδιάμεσου, εξόδου), κάτι που αυξάνει την καθυστέρηση μετάδοσης.

Q8: Τι σημαίνει η κατάληξη domain .onion;

Είναι ένα εξειδικευμένο επίθημα τομέα ανωτάτου επιπέδου που χρησιμοποιείται στα δίκτυα Tor, δείχνοντας σε κρυπτογραφικά παραγόμενες διευθύνσεις αντί για τυπικούς διακομιστές DNS.

Q9: Ποιοι κίνδυνοι συνδέονται με τους συνδέσμους του dark web;

Οι ιστότοποι δεν έχουν έλεγχο ασφαλείας, εκθέτοντας τους χρήστες σε υψηλά ποσοστά μόλυνσης από κακόβουλο λογισμικό, σενάρια ηλεκτρονικού ψαρέματος (phishing) και απάτες συναλλαγών.

Q10: Ποιος δημιούργησε το πρωτόκολλο δρομολόγησης του δικτύου Tor;

Η τεχνολογία αναπτύχθηκε αρχικά από το Ναυτικό Ερευνητικό Εργαστήριο των ΗΠΑ τη δεκαετία του 1990 για την προστασία κυβερνητικών επικοινωνιών.

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 προστατεύουν οι ενδιάμεσοι κόμβοι την ανωνυμία στο Tor;

Κάθε κόμβος αποκρυπτογραφεί μόνο ένα επίπεδο δεδομένων δρομολόγησης, μαθαίνοντας μόνο το προηγούμενο και το επόμενο άλμα, ποτέ και την πηγή και τον προορισμό μαζί.

Q2: Ποιος είναι ο ρόλος του κόμβου εξόδου;

Ο κόμβος εξόδου αποκρυπτογραφεί το τελευταίο επίπεδο κρυπτογράφησης, στέλνοντας την κίνηση προς τον δημόσιο διακομιστή προορισμού ή τον διακομιστή onion.

Q3: Τι είναι μια πύλη γεφυρών Tor;

Οι γέφυρες (bridges) είναι μη καταχωρισμένοι κόμβοι εισόδου Tor που χρησιμοποιούνται για την παράκαμψη αποκλεισμών του ISP και της λογοκρισίας σε περιοχές που περιορίζουν την πρόσβαση στο πρόγραμμα περιήγησης Tor.

Q4: Πώς εκμεταλλεύονται τα κρυπτονομίσματα οι δράστες του dark web;

Οι δράστες χρησιμοποιούν ανώνυμα κρυπτονομίσματα για να εκτελούν οικονομικές συναλλαγές σε σκοτεινές αγορές, παρακάμπτοντας τους τυπικούς τραπεζικούς ελέγχους συναλλαγών.

Q5: Γιατί οι κοινές μηχανές αναζήτησης αδυνατούν να ανιχνεύσουν βαθιές βάσεις δεδομένων;

Τα ρομπότ ανίχνευσης (crawlers) δεν μπορούν να εισάγουν διαπιστευτήρια σύνδεσης, να λύσουν CAPTCHA ασφαλείας ή να εκτελέσουν σενάρια ερωτημάτων SQL στο παρασκήνιο που απαιτούνται για την πρόσβαση σε βαθιές βάσεις δεδομένων.

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: Τι είναι ένας διακομιστής καταλόγου στα δίκτυα Tor;

Είναι ένας αξιόπιστος διακομιστής που τηρεί τη λίστα των ενεργών ρελέ εισόδου, μέσου και εξόδου που χρησιμοποιούν οι πελάτες για να κατασκευάσουν διαδρομές δρομολόγησης.

Q7: Πώς εκτελούν κακόβουλοι δράστες υποκλοπή σε κόμβους εξόδου (exit node sniffing);

Οι χειριστές κακόβουλων κόμβων εξόδου μπορούν να υποκλέψουν μη κρυπτογραφημένη κίνηση HTTP καθώς εγκαταλείπει το δίκτυο Tor, κλέβοντας ονόματα χρηστών και cookies.

Q8: Ποια είναι η διαφορά μεταξύ Tor και I2P;

Το Tor χρησιμοποιεί κεντρικό κατάλογο κόμβων αναμετάδοσης και κόμβους εξόδου για πρόσβαση στον δημόσιο ιστό, ενώ το I2P χρησιμοποιεί αποκεντρωμένη δομή ομότιμων κόμβων (peer-to-peer) για εσωτερική φιλοξενία.

Q9: Πώς εντοπίζουν οι υπηρεσίες επιβολής του νόμου τις αγορές του dark web;

Οι υπηρεσίες χρησιμοποιούν ανάλυση blockchain, εντοπίζουν φυσικές εγκαταστάσεις φιλοξενίας διακομιστών και διεξάγουν επιχειρήσεις-δολώματα για να εντοπίσουν τους διαχειριστές.

Q10: Πώς θέτει σε κίνδυνο η διαρροή DNS την ανωνυμία του πελάτη;

Οι διαρροές DNS συμβαίνουν όταν τα ερωτήματα DNS του προγράμματος περιήγησης στέλνονται απευθείας μέσω του τοπικού παρόχου αντί να δρομολογούνται μέσω του κρυπτογραφημένου δικτύου Tor.

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

Το deep web είναι πολύ μεγαλύτερο από το επιφανειακό web που αναζητείται, καθώς το μεγαλύτερο μέρος του περιεχομένου βρίσκεται πίσω από συνδέσεις και βάσεις δεδομένων.

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το dark web είναι ένα μικρό, σκόπιμα κρυμμένο τμήμα του deep web, στο οποίο φτάνεις με εργαλεία όπως το Tor.

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η δρομολόγηση Tor κρυπτογραφεί τα πακέτα δεδομένων τρεις φορές, αφαιρώντας επίπεδα κρυπτογράφησης σαν φλούδες κρεμμυδιού σε κάθε κόμβο αναμετάδοσης.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το Tor προέκυψε από το έργο δρομολόγησης onion του Ναυτικού Ερευνητικού Εργαστηρίου των ΗΠΑ και ο κώδικάς του δημοσιεύθηκε ως ελεύθερο λογισμικό. [1]

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι διευθύνσεις onion είναι αλφαριθμητικές συμβολοσειρές 56 χαρακτήρων που παράγονται κρυπτογραφικά από ζεύγη δημόσιων κλειδιών.

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι κόμβοι εξόδου μπορούν να διαβάσουν κίνηση σε απλό κείμενο, πράγμα που σημαίνει ότι το TLS/HTTPS εξακολουθεί να απαιτείται στο Tor για ασφαλή δεδομένα συνεδρίας.

7. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι ιστότοποι ενδοδικτύου, οι μονάδες cloud και οι ιδιωτικές βάσεις δεδομένων αποτελούν τα μεγαλύτερα τμήματα αποθήκευσης δεδομένων στο deep web.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Εξειδικευμένες μηχανές αναζήτησης όπως το DuckDuckGo διατηρούν πύλες onion που επιτρέπουν ανώνυμες αναζητήσεις στα δίκτυα Tor.

9. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Πάνω από 2 εκατομμύρια χρήστες συνδέονται καθημερινά στο δίκτυο Tor για να παρακάμψουν τη λογοκρισία και να διατηρήσουν την ιδιωτικότητα των επικοινωνιών τους.

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Παγκόσμιες επιχειρήσεις των αρχών επιβολής του νόμου (όπως η Operation Bayonet) έκλεισαν μεγάλες αγορές του dark web κατάσχοντας το υλικό φιλοξενίας.

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] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] 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

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 **Ευρετηρίαση αναζήτησης** ΒΑΘΥΣ ΙΣΤΟΣ — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι σελίδες του βαθέος ιστού βρίσκονται πίσω από τοίχους σύνδεσης και βάσεις δεδομένων, εμποδίζοντας τους ανιχνευτές των μηχανών αναζήτησης να τις σαρώσουν. Παραπομπή: IETF RFC 3986.

2 **Πρόσβαση στο Tor** ΣΚΟΤΕΙΝΟΣ ΙΣΤΟΣ — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το dark web αποτελείται από κρυφές υπηρεσίες onion στις οποίες έχεις πρόσβαση μόνο μέσω προγραμμάτων περιήγησης όπως το Tor. Παραπομπή: IETF RFC 3986.

3 **Βαθιές βάσεις δεδομένων** ΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι λογαριασμοί με κωδικό πρόσβασης και τα εταιρικά αρχεία αποτελούν το μεγαλύτερο τμήμα του deep web. Παραπομπή: NIST Digital Identity.

4 **Δρομολόγηση Onion** ΔΙΚΤΥΟ TOR — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η δρομολόγηση onion κρυπτογραφεί τα πακέτα δεδομένων σε επίπεδα και τα αναμεταδίδει μέσω πολλών κόμβων για ανωνυμία. Παραπομπή: IETF RFC 3986.

5 **Τομέας Onion** ΚΑΤΑΛΗΞΗ — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το κρυπτογραφικό επίθημα τομέα.onion δρομολογεί την κίνηση εσωτερικά στο Tor χωρίς δημόσιο DNS. Παραπομπή: IETF RFC 3986.

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 **Τμήματα ιστού** ΔΟΜΗ — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το deep web καλύπτει όλες τις μη ευρετηριασμένες σελίδες, ενώ το dark web είναι ένα μικρό, κρυπτογραφημένο υποτμήμα onion. Παραπομπή: IETF RFC 3986. [1]

7 **Εταιρικά intranet** ΒΑΘΥΣ ΙΣΤΟΣ — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι ιστότοποι ενδοδικτύου βρίσκονται πίσω από πύλες με κωδικό πρόσβασης και δεν δεικτοδοτούνται, πράγμα που σημαίνει ότι ανήκουν στο βαθύ διαδίκτυο (deep web). Παραπομπή: NIST Digital Identity.

8 **Κρυπτογράφηση ανά επίπεδο** ΚΟΜΒΟΙ RELAY — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι κόμβοι onion αποκρυπτογραφούν μόνο ένα επίπεδο δρομολόγησης για να προστατεύουν την ανωνυμία του χρήστη, ποτέ ολόκληρο το πακέτο. Παραπομπή: IETF RFC 3986.

9 **Έκθεση σε κακόβουλο λογισμικό** ΑΠΕΙΛΕΣ — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι αγορές του σκοτεινού ιστού δεν έχουν φιλτράρισμα ασφάλειας και ενέχουν ακραίους κινδύνους μόλυνσης από κακόβουλο λογισμικό. Παραπομπή: Center for Internet Security (CIS).

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

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι συνηθισμένοι ανιχνευτές των μηχανών αναζήτησης δεν χρησιμοποιούν το Tor, οπότε δεν μπορούν να φτάσουν ή να ευρετηριάσουν ιστότοπους .onion.

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. Τμήμα του βαθέος διαδικτύου (Deep Web)	A 2. Πύλη Dark Web	D 3. Επέκταση Onion	B 4. Δρομολόγηση Tor
F 5. Ευρετηριασμένες σελίδες	G 6. Ανωνυμία χρήστη	C 7. Ιδιωτική βάση δεδομένων	E 8. Πύλη εισόδου

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΒΑΘΥΣ ΙΣΤΟΣ	2 ΣΚΟΤΕΙΝΟΣ ΙΣΤΟΣ	3 ONION	4 ΔΡΟΜΟΛΟΓΗΣΗ
5 ΑΝΑΖΗΤΗΣΙΜΕΣ	6 ΑΝΩΝΥΜΙΑ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 F – ΑΝΩΝΥΜΙΑ	2 G – ΒΑΣΗΔΕΔΟΜΕΝΩΝ	3 D – ΔΡΟΜΟΛΟΓΗΣΗ	4 A – ΒΑΘΥΣΙΣΤΟΣ
5 B – ΣΚΟΤΕΙΝΟΣΙΣΤΟΣ	6 C – ΚΡΕΜΜΥΔΙ	7 H – ΚΟΜΒΟΣ	8 E – ΑΝΑΖΗΤΗΣΙΜΕΣ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

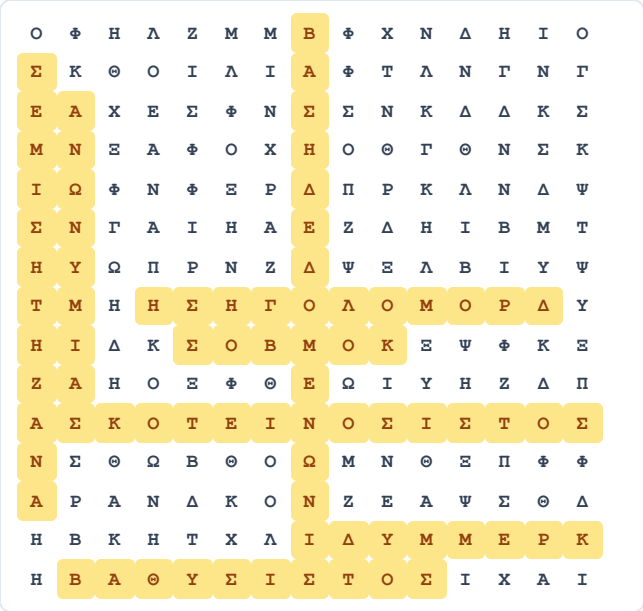
Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους Τμήμα του βαθέος διαδικτύου (Deep Web), Πύλη Dark Web και Επέκταση Onion και να δώσουν ένα παράδειγμα για τον καθένα.

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

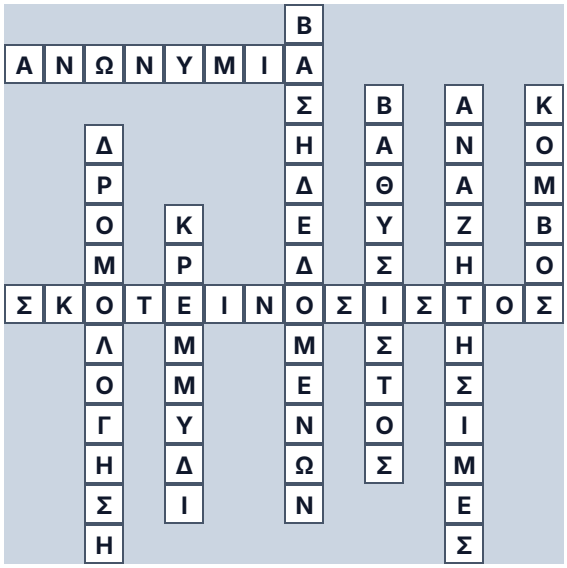
Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ



ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ



ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

2 οριζόντια: ΑΝΩΝΥΜΙΑ Απόκρυψη των δημόσιων διευθύνσεων IP των πελατών από τους διακομιστές (8 γράμματα)

8 οριζόντια: ΣΚΟΤΕΙΝΟΣΙΣΤΟΣ Κρυπτογραφημένο τμήμα δικτύου που είναι προσβάσιμο μόνο μέσω ειδικών προγραμμάτων περιήγησης (14 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΒΑΣΗΔΕΔΟΜΕΝΩΝ Ασφαλής αποθήκευση στο παρασκήνιο που φιλοξενεί εγγραφές συστήματος χωρίς ευρετηρίαση (13 γράμματα)

3 κάθετα: ΒΑΘΥΣΙΣΤΟΣ Περιεχόμενο ιστού χωρίς ευρετηρίαση, όπως ιδιωτικές συνδέσεις, email και εγγραφές βάσεων δεδομένων (10 γράμματα)

4 κάθετα: ΑΝΑΖΗΤΗΣΙΜΕΣ Περιεχόμενο του ιστού της επιφάνειας που έχει καταγραφεί και είναι αναζητήσιμο στο Google (12 γράμματα)

5 κάθετα: ΚΟΜΒΟΣ Ο κόμβος εισόδου που χρησιμοποιείται για πρόσβαση στο δίκτυο Tor (6 γράμματα)

6 κάθετα: ΔΡΟΜΟΛΟΓΗΣΗ Κρυπτογράφηση των δεδομένων σε επίπεδα και αναμετάδοσή τους μέσω τριών κόμβων (11 γράμματα)

7 κάθετα: ΚΡΕΜΜΥΔΙ Λαχανικό με επάλληλα στρώματα, από το οποίο παίρνει το όνομά της η κατάληξη των κρυφών υπηρεσιών του Tor (8 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

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

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΟΣΙΣΑΒΤΣΥΘ — **ΒΑΘΥΣΙΣΤΟΣ**
2. ΜΚΙΡΔΥΜΕ — **ΚΡΕΜΜΥΔΙ**
3. ΑΝΣΗΕΙΑΤΣΗΜΖ — **ΑΝΑΖΗΤΗΣΙΜΕΣ**
4. ΕΩΜΣΟΔΝΔΝΕΒΑΗ — **ΒΑΣΗΔΕΔΟΜΕΝΩΝ**
5. ΙΟΤΚΟΣΕΣΙΣΝΣΟΤ — **ΣΚΟΤΕΙΝΟΣΙΣΤΟΣ**
6. ΟΗΛΓΣΗΔΡΟΟΜ — **ΔΡΟΜΟΛΟΓΗΣΗ**
7. ΑΑΥΜΙΝΝΩ — **ΑΝΩΝΥΜΙΑ**
8. ΜΣΚΟΒΟ — **ΚΟΜΒΟΣ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΔΙΑΤΗΡΗΣΕ ΤΗΝ ΑΝΩΝΥΜΙΑ ΜΕ ΑΣΦΑΛΗ ΔΡΟΜΟΛΟΓΗΣΗ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Εντοπισμός διαρροής δεδομένων

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένας εταιρικός έλεγχος ασφαλείας ανακαλύπτει ότι εγγραφές ευαίσθητων βάσεων δεδομένων πελατών διακινούνται σε αγορά onion. Τα δεδομένα δεν έχουν ευρετηριαστεί στη Google.
- Προτεινόμενη στρατηγική και λύση: Εμπλεκόμενα τμήματα: Η ιδιωτική βάση δεδομένων ανήκει στο deep web (χωρίς ευρετηρίαση αλλά ασφαλής). Η αγορά που διακινεί τα κλεμμένα δεδομένα βρίσκεται στο dark web (δίκτυο onion). Πώς έγινε: Οι χάκερ παρέκαμψαν τις άμυνες του διακομιστή, έκλεψαν τη βάση δεδομένων από το deep web και την ανάρτησαν ανώνυμα στο dark web για να ξεφύγουν από την παρακολούθηση των αρχών.

B Μελέτη περίπτωσης 2: Ανωνυμία έναντι κινδύνων κακόβουλου λογισμικού

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένας αναλυτής θέλει να ελέγξει ροές πληροφοριών απειλών σε ιστότοπο Tor. Κατεβάζει το πρόγραμμα περιήγησης Tor και μπαίνει στον ιστότοπο.
- Προτεινόμενη στρατηγική και λύση: Οφέλη: Το Tor δρομολογεί την κίνηση μέσω τριών κόμβων, κρύβοντας την εταιρική IP του αναλυτή. Κίνδυνοι και μετριασμός: Οι σύνδεσμοι του dark web δεν έχουν έλεγχο φήμης. Οι αναλυτές πρέπει να εκτελούν το Tor μέσα σε απομονωμένες εικονικές μηχανές (VM), να απενεργοποιούν τη JavaScript στις ρυθμίσεις του Tor και να αποφεύγουν τη λήψη οποιωνδήποτε αρχείων για να προστατεύσουν το εταιρικό δίκτυο.