

ΘΕΜΑΤΑ ΕΞΕΤΑΣΕΩΝ

ΠΙΣΤΟΠΟΙΗΣΗΣ ΑΠΟΦΟΙΤΩΝ ΕΠΑ.Σ. ΜΑΘΗΤΕΙΑΣ ΚΑΙ Π.ΕΠΑ.Σ. ΜΑΘΗΤΕΙΑΣ της Δ.ΥΠ.Α.

ΕΙΔΙΚΟΤΗΤΑ ΕΠΑ.Σ.: “ Υπάλληλος
Υποστήριξης Συστημάτων
Κυβερνοασφάλειας”

ΠΕΡΙΕΧΟΜΕΝΑ

- 1.** Θεσμικό Πλαίσιο Εξετάσεων Πιστοποίησης των αποφοίτων ΕΠΑ.Σ. Μαθητείας και Π.ΕΠΑ.Σ. Μαθητείας της Δημόσιας Υπηρεσίας Απασχόλησης (Δ.ΥΠ.Α.)
- 2.** Κατάλογος Ερωτήσεων Θεωρητικής Κατεύθυνσης
- 3.** Κατάλογος Ερωτήσεων Πρακτικής Κατεύθυνσης
- 4.** Απαντήσεις Ερωτήσεων Θεωρητικής Κατεύθυνσης
- 5.** Απαντήσεις Ερωτήσεων Πρακτικής Κατεύθυνσης

1.Θεσμικό Πλαίσιο Εξετάσεων Πιστοποίησης των αποφοίτων ΕΠΑ.Σ. Μαθητείας και Π.ΕΠΑ.Σ. Μαθητείας της Δημόσιας Υπηρεσίας Απασχόλησης (Δ.ΥΠ.Α.)

Οι Εξετάσεις Πιστοποίησης των αποφοίτων ΕΠΑ.Σ. Μαθητείας και Π.ΕΠΑ.Σ. Μαθητείας της Δημόσιας Υπηρεσίας Απασχόλησης (Δ.ΥΠ.Α.) της ειδικότητας «**Υπάλληλος Υποστήριξης Συστημάτων Κυβερνοασφάλειας**» διεξάγονται σύμφωνα με τα οριζόμενα στις διατάξεις της υπ' αριθμ. 51/κ6/29.12.2023 (ΦΕΚ 1/Β/2.1.2024) Κοινής Υπουργικής Απόφασης Εθνικής Οικονομίας και Οικονομικών και Παιδείας Θρησκευμάτων και Αθλητισμού.

2. ΕΡΩΤΗΣΕΙΣ ΘΕΩΡΗΤΙΚΗΣ ΚΑΤΕΥΘΥΝΣΗΣ

ΚΑΤΑΛΟΓΟΣ ΕΡΩΤΗΣΕΩΝ ΠΟΛΛΑΠΛΗΣ ΕΠΙΛΟΓΗΣ ΓΙΑ ΤΗΝ ΑΠΟΤΙΜΗΣΗ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ

1		Τι είναι η Ασφάλεια Πληροφοριακών Συστημάτων		
	α.	Η προστασία μόνο από φυσικούς κινδύνους		
	β.	Η εξασφάλιση της ακεραιότητας των δεδομένων		
	γ.	Η προστασία από κινδύνους που αφορούν την πληροφορία και τα συστήματα που την επεξεργάζονται		
	δ.	Η εξασφάλιση της διαθεσιμότητας μόνο των δεδομένων		
2		Τι αναφέρεται στη διαδικασία επιβεβαίωσης της ταυτότητας ενός χρήστη σε ένα πληροφοριακό σύστημα;		
	α.	Κοινωνική Μηχανική		
	β.	Απειλές κατά των Δεδομένων		
	γ.	Πιστοποίηση Ταυτότητας		
	δ.	Χάκερς		

3		Πώς ορίζεται η Πιστοποίηση Ταυτότητας στο πλαίσιο της ασφάλειας πληροφοριακών συστημάτων;		
	α.	Η προστασία των δεδομένων από ανεπιθύμητη πρόσβαση		
	β.	Η διαδικασία επαλήθευσης της αυθεντικότητας ενός χρήστη		
	γ.	Η πρόληψη από ηλεκτρονικό έγκλημα		
	δ.	Η προστασία από κακόβουλο λογισμικό		
4		Ποια από τα παρακάτω αναφέρεται στη διατήρηση της ακεραιότητας των δεδομένων;		
	α.	Ηλεκτρονικό Έγκλημα		
	β.	Πιστοποίηση Ταυτότητας		
	γ.	Ακεραιότητα		
	δ.	Κοινωνική Μηχανική		
5		Πώς ορίζεται η Κοινωνική Μηχανική;		
	α.	Η αναγνώριση των κινδύνων από τον άνθρωπο		
	β.	Η χρήση τεχνικών για την απόκτηση πληροφοριών από ανθρώπους		
	γ.	Η αυτόματη προστασία των δεδομένων		
	δ.	Η διαδικασία επαλήθευσης της ταυτότητας		
6		Ποιο από τα παρακάτω ισχύει για την εμπιστευτικότητα των δεδομένων;		
	α.	Η διατήρηση της ακεραιότητας		
	β.	Η προστασία από απώλεια δεδομένων		
	γ.	Η διασφάλιση ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση		
	δ.	Η διατήρηση του αναλώσιμου χώρου αποθήκευσης		
7		Ποια είναι η ορισμός του Ηλεκτρονικού Έγκληματος;		

	α.	Η παράνομη χρήση του Διαδικτύου		
	β.	Κάθε παράνομη δραστηριότητα που συμβαίνει online		
	γ.	Η παράνομη χρήση της τεχνολογίας για τη διάπραξη εγκλημάτων		
	δ.	Κάθε παράνομη δραστηριότητα που συμβαίνει offline		
8		Ποια από τα παρακάτω αναφέρεται στις απειλές κατά των δεδομένων;		
	α.	Πιστοποίηση Ταυτότητας		
	β.	Χάκερς		
	γ.	Ασφάλεια Πληροφοριακών Συστημάτων		
	δ.	Ακεραιότητα		
9		Ποια από τα παρακάτω αναφέρεται στην διατήρηση της διαθεσιμότητας των δεδομένων;		
	α.	Ακεραιότητα		
	β.	Εμπιστευτικότητα		
	γ.	Ηλεκτρονικό Έγκλημα		
	δ.	Διαθεσιμότητα		
10		Τι περιλαμβάνει η διαδικασία της εξουσιοδότησης σε ένα πληροφοριακό σύστημα;		
	α.	Έλεγχο της κυκλοφορίας των δεδομένων		
	β.	Επαλήθευση της ταυτότητας ενός χρήστη		
	γ.	Καθορισμός των δικαιωμάτων πρόσβασης		
	δ.	Προστασία από κακόβουλο λογισμικό		
11		Τι είναι η κρυπτογράφηση;		
	α.	Η διαδικασία δημιουργίας κρυφών μηνυμάτων		
	β.	Η διαδικασία ανάκτησης δεδομένων		
	γ.	Η διαδικασία αποστολής email		

	δ.	Η διαδικασία συντήρησης υπολογιστών		
12		Ποιος είναι ο σκοπός της αυθεντικοποίησης;		
	α.	Να ελέγχει την ταχύτητα του δικτύου		
	β.	Να επιβεβαιώνει την ταυτότητα ενός χρήστη		
	γ.	Να αποθηκεύει αρχεία στον σκληρό δίσκο		
	δ.	Να καθαρίζει ιούς από το σύστημα		
13		Τι είναι ένας ιός υπολογιστή;		
	α.	Ένα πρόγραμμα που βοηθά στην αυτόματη ενημέρωση του λογισμικού		
	β.	Ένα πρόγραμμα που προστατεύει από κακόβουλο λογισμικό		
	γ.	Ένα κακόβουλο πρόγραμμα που μπορεί να προκαλέσει ζημιά σε έναν υπολογιστή		
	δ.	Ένα εργαλείο για την επισκευή του υπολογιστή		
14		Τι είναι ένα τείχος προστασίας (firewall);		
	α.	Ένα πρόγραμμα για τη δημιουργία αντιγράφων ασφαλείας		
	β.	Ένα δίκτυο που συνδέει υπολογιστές σε όλο τον κόσμο		
	γ.	Ένα σύστημα που προστατεύει ένα δίκτυο από μη εξουσιοδοτημένη πρόσβαση		
	δ.	Ένα εργαλείο για την ανάλυση δεδομένων		
15		Τι είναι η ασφάλεια δικτύου;		
	α.	Η προστασία των δεδομένων κατά τη μεταφορά τους σε ένα δίκτυο		
	β.	Η διαδικασία εγκατάστασης δικτυακού εξοπλισμού		
	γ.	Η ταχύτητα μεταφοράς δεδομένων σε ένα δίκτυο		
	δ.	Η διαδικασία δημιουργίας δικτυακών καλωδίων		

16		Τι είναι το firewall σε ένα δίκτυο;		
	α.	Ένα φυσικό τοίχος προστασίας.		
	β.	Ένα πρόγραμμα που ελέγχει την είσοδο και έξοδο δεδομένων.		
	γ.	Ένας τύπος καλωδίου δικτύου.		
	δ.	Ένα είδος ιού.		
17		Τι είναι το malware;		
	α.	Ένα πρόγραμμα που προστατεύει τον υπολογιστή.		
	β.	Κακόβουλο λογισμικό που προκαλεί ζημιά.		
	γ.	Ένας τύπος firewall.		
	δ.	Ένα είδος κωδικοποιητή.		
18		Τί είναι ο προγραμματισμός;		
	α.	Η διαδικασία εκτέλεσης εφαρμογών.		
	β.	Η δημιουργία λογισμικού μέσω μιας γλώσσας προγραμματισμού.		
	γ.	Η ανάπτυξη hardware.		
	δ.	Η συντήρηση υπολογιστικών συστημάτων.		
19		Τί είναι η μεταβλητή σε ένα πρόγραμμα;		
	α.	Ένα αντικείμενο που καταναλώνει μνήμη.		
	β.	Ένα τμήμα κώδικα που εκτελεί μια συγκεκριμένη λειτουργία.		
	γ.	Ένα όνομα που χρησιμοποιείται για να αναφερθεί σε μια τιμή ή θέση μνήμης.		
	δ.	Ένα πρόγραμμα εκτέλεσης.		

20		Τί ονομάζεται πηγαίος κώδικας σε ένα πρόγραμμα;		
	α.	Ένα εκτελέσιμο αρχείο.		
	β.	Ο κώδικας που γράφεται από τον προγραμματιστή.		
	γ.	Ένα είδος μεταβλητής.		
	δ.	Η είσοδος του προγράμματος.		
21		Τί σημαίνει ο όρος "συντακτικό σφάλμα" σε ένα πρόγραμμα;		
	α.	Ένα σφάλμα στην εκτέλεση του προγράμματος.		
	β.	Ένα σφάλμα στη σύνταξη του κώδικα.		
	γ.	Ένα σφάλμα στη λογική του προγράμματος.		
	δ.	Ένα σφάλμα στην αποθήκευση δεδομένων.		
22		Τί αναπαριστά ένας αλγόριθμος;		
	α.	Ένα είδος βάσης δεδομένων.		
	β.	Ο τρόπος εκτέλεσης και τα βήματα που πρέπει να ακολουθηθούν για την εκτέλεση μιας εργασίας.		
	γ.	Ένα είδος μεταβλητής.		
	δ.	Η ανταλλαγή δεδομένων μεταξύ προγραμμάτων.		
23		Τί είναι η δομή ελέγχου "if-else" (εάν-τότε);		
	α.	Ένας τρόπος εκτέλεσης ενός τμήματος κώδικα επαναληπτικά.		
	β.	Ένας τύπος μεταβλητής.		
	γ.	Μια δομή που επιτρέπει τον έλεγχο μιας συνθήκης και την εκτέλεση διαφορετικού κώδικα ανάλογα με το αποτέλεσμα.		
	δ.	Ένα είδος μεταγλωττιστή.		
24		Τί είναι το "debugging" (αποσφαλμάτωση) στον προγραμματισμό;		

	α.	Η δημιουργία του τελικού εκτελέσιμου αρχείου.		
	β.	Η διαγραφή του κώδικα.		
	γ.	Η διαδικασία εύρεσης και διόρθωσης σφαλμάτων στον κώδικα.		
	δ.	Η αναζήτηση νέων ιδεών για τη βελτίωση του προγράμματος.		
25		Τί είναι το "loop" (επανάληψη) στον προγραμματισμό;		
	α.	Ένα αντικείμενο.		
	β.	Ένας τύπος μεταβλητής.		
	γ.	Ένας τρόπος εκτέλεσης ενός τμήματος κώδικα επαναληπτικά.		
	δ.	Ένα πρόγραμμα εκτέλεσης.		
26		Τί ονομάζεται συντακτικό στον προγραμματισμό;		
	α.	Ένας τρόπος ανάκτησης δεδομένων.		
	β.	Ένας τύπος μεταβλητής.		
	γ.	Η σωστή δομή ενός προγράμματος γλώσσας προγραμματισμού.		
	δ.	Ένα είδος αλγορίθμου.		
27		Τι είναι η συνάρτηση σε ένα πρόγραμμα;		
	α.	Ένα είδος μεταβλητής.		
	β.	Ένα τμήμα κώδικα που εκτελεί μια συγκεκριμένη λειτουργία και μπορεί να καλείται από άλλα τμήματα του προγράμματος.		
	γ.	Ένα είδος δομής ελέγχου.		
	δ.	Ο κώδικας σε δυαδική μορφή.		
28		Τι είναι η κρυπτογραφία;		
	α.	Η επιστήμη που ασχολείται με τη μελέτη των κρυμμένων θησαυρών.		

	β.	Η τέχνη κρυφής γραφής και αποκρυπτογράφησης πληροφοριών.		
	γ.	Η επιστήμη της ασφάλειας στο Διαδίκτυο.		
	δ.	Ένα είδος αντικειμένου για συλλέκτες.		
29		Ποιος είναι ο σκοπός της κρυπτογραφίας;		
	α.	Να προστατεύει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των πληροφοριών.		
	β.	Να δημιουργεί κώδικα.		
	γ.	Να προστατεύει την ασφάλεια του Διαδικτύου.		
	δ.	Κανένα από τα παραπάνω.		
30		Ποιο από τα παρακάτω ΔΕΝ ανήκει στις βασικές κατηγορίες κρυπτογραφίας;		
	α.	Κρυπτογραφία κλειδιού (Symmetric Cryptography).		
	β.	Κρυπτογραφία ροής (Stream Cipher).		
	γ.	Κρυπτογραφία λογισμικού.		
	δ.	Κρυπτογραφία κειμένου (Public Key Cryptography ή Asymmetric Cryptography).		
31		Τι είναι το κλειδί κρυπτογράφησης;		
	α.	Μια σειρά ψηφίων ή χαρακτήρων που χρησιμοποιείται για την ανταλλαγή μηνυμάτων.		
	β.	Ένα πρόγραμμα υπολογιστή για κρυπτογραφία.		
	γ.	Ένας αλγόριθμος για την αποκρυπτογράφηση δεδομένων.		
	δ.	Ένα μυστικό κλειδί που χρησιμοποιείται στη διαδικασία κρυπτογράφησης.		
32		Τι είναι το SSL/TLS;		
	α.	Ένα πρωτόκολλο κρυπτογράφησης που χρησιμοποιείται για ασφαλείς συνδέσεις στο Διαδίκτυο.		
	β.	Ένα λογισμικό για ανάλυση κρυπτογραφημένων αρχείων.		
	γ.	Ένα είδος αλγορίθμου κρυπτογράφησης.		
	δ.	Ένα πακέτο λογισμικού για τη διαχείριση κλειδιών.		

33		Ποιος είναι ο κύριος στόχος της δημόσιας κρυπτογραφίας;		
	α.	Η κρυπτογράφηση μηνυμάτων μόνο από ειδικούς.		
	β.	Η κρυπτογράφηση μηνυμάτων μόνο για στρατιωτική χρήση.		
	γ.	Η κρυπτογράφηση μηνυμάτων που μπορούν να αποκρυπτογραφηθούν από οποιονδήποτε.		
	δ.	Η κρυπτογράφηση μόνο για την προστασία των τραπεζικών δεδομένων.		
34		Ποιος αλγόριθμος κρυπτογραφίας είναι γνωστός για τη δυνατότητά του να αποκρυπτογραφήσει τα δεδομένα μόνο με ένα κλειδί;		
	α.	Κρυπτογραφία με δημόσιο κλειδί.		
	β.	Κρυπτογραφία με συμμετρικό κλειδί.		
	γ.	Κρυπτογραφία με διπλό κλειδί.		
	δ.	Κρυπτογραφία με ασύμμετρο κλειδί.		
35		Ποια από τις παρακάτω είναι μια από τις βασικές αρχές της κρυπτογραφίας;		
	α.	Οποιοσδήποτε μπορεί να αποκρυπτογραφήσει τα δεδομένα.		
	β.	Ο κρυπταναλυτής πρέπει να έχει εξειδικευμένες γνώσεις για να αποκρυπτογραφήσει τα δεδομένα.		
	γ.	Ο κρυπταναλυτής πρέπει να μπορεί να αποκρυπτογραφήσει τα δεδομένα μόνο με το κλειδί.		
	δ.	Η κρυπτογραφία δεν είναι ασφαλής μέθοδος προστασίας των δεδομένων.		
36		Ποιο από τα παρακάτω δεν είναι ένα από τα βασικά αρχέγονα μέτρα ασφαλείας στην κυβερνοασφάλεια;		
	α.	Ανίχνευση εισβολής		
	β.	Κρυπτογράφηση δεδομένων		
	γ.	Προστασία με κωδικό πρόσβασης		
	δ.	Διαχείριση αντιγράφων ασφαλείας		

37		Ποιος από τους παρακάτω ορίζει την πολιτική ασφαλείας και τους κανόνες πρόσβασης σε ένα δίκτυο;		
	α.	Καταναλωτής		
	β.	Επιτροπή ασφαλείας		
	γ.	Διαχειριστής		
	δ.	Επιθετικός χάκερ		
38		Ποιο από τα παρακάτω είναι ένα είδος κακόβουλου λογισμικού που κλέβει προσωπικές πληροφορίες χρησιμοποιώντας παραπλανητικές τεχνικές;		
	α.	Firewall		
	β.	Trojan		
	γ.	VPN		
	δ.	DNS		
39		Ποιος από τους παρακάτω είναι ένας τύπος επίθεσης κυβερνοασφάλειας που στοχεύει στο να εξαναγκάσει ένα υπολογιστικό σύστημα να υποκλιθεί σε ανεπιθύμητες ενέργειες;		
	α.	Brute Force Attack		
	β.	Malware		
	γ.	Denial of Service (DoS) Attack		
	δ.	Firewall		
40		Ποιο από τα παρακάτω αποτελεί πρωτόκολλο που χρησιμοποιείται συνήθως για την ασφαλή απομακρυσμένη σύνδεση σε ένα δίκτυο;		
	α.	DNS		
	β.	HTTP		
	γ.	SSL/TLS		
	δ.	SNMP		
41		Ποιο από τα παρακάτω ΔΕΝ είναι ένα βασικό στοιχείο ενός υπολογιστικού συστήματος;		
	α.	Επεξεργαστής (CPU)		

	β.	Σκληρός δίσκος (Hard Drive)		
	γ.	Ποντίκι (Mouse)		
	δ.	Μνήμη RAM (RAM)		
42		Ποιος από τους παρακάτω αποτελεί γλώσσα προγραμματισμού;		
	α.	Windows		
	β.	Microsoft Office		
	γ.	Python		
	δ.	Adobe Photoshop		
43		Ποιο από τα παρακάτω ΔΕΝ ανήκει στις βασικές επικοινωνιακές τεχνολογίες στο Διαδίκτυο;		
	α.	HTTP		
	β.	FTP		
	γ.	MP3		
	δ.	TCP/IP		
44		Ποιος είναι ο ρόλος ενός λειτουργικού συστήματος;		
	α.	Να επεξεργάζεται δεδομένα		
	β.	Να παρέχει πρόσβαση στο Διαδίκτυο		
	γ.	Να διαχειρίζεται τους πόρους του υπολογιστή και να εκτελεί εφαρμογές		
	δ.	Να δημιουργεί γραφικά σχέδια		
45		Τι σημαίνει το ακρωνύμιο "SSL";		
	α.	Secure Sockets Layer		
	β.	Safe Software Language		
	γ.	System Security Level		
	δ.	Strong System Language		

46		Τι αποτελεί πληροφορία;		
	α.	Ένας αριθμός		
	β.	Ένα γράμμα		
	γ.	Ένας συνδυασμός δεδομένων με νόημα		
	δ.	Ένα ηλεκτρονικό κύκλωμα		
47		Ποιο από τα παρακάτω ΔΕΝ είναι ένα είδος δεδομένων;		
	α.	a. Κείμενο		
	β.	b. Εικόνα		
	γ.	c. Ήχος		
	δ.	d. Κινητό τηλέφωνο		
48		Ποια είναι η βασική λειτουργία ενός λειτουργικού συστήματος υπολογιστών;		
	α.	Εκτέλεση επεξεργαστικών εργασιών		
	β.	Εκτέλεση εφαρμογών		
	γ.	Διαχείριση πόρων και υπηρεσιών		
	δ.	Αποθήκευση αρχείων		
49		Ποιο από τα παρακάτω χαρακτηριστικά ΔΕΝ ανήκει στα γνωρίσματα ενός λειτουργικού συστήματος;		
	α.	Πολυεργασία		
	β.	Πολυεπεξεργασία		
	γ.	Πολλαπλές επιφάνειες εργασίας		
	δ.	Ζωγραφική		
50		Τι είναι ένας πυρήνας (kernel) σε ένα λειτουργικό σύστημα;		
	α.	Ένα πρόγραμμα περιήγησης στον ιστό		

	β.	Ένας βασικός χρήστης του συστήματος		
	γ.	Ο κεντρικός πυρήνας υπολογιστή		
	δ.	Ο πυρήνας που διαχειρίζεται την επικοινωνία με το υλικό και τις βασικές λειτουργίες του λειτουργικού συστήματος		
51		Ποια είναι η λειτουργία της διαχείρισης μνήμης σε ένα λειτουργικό σύστημα;		
	α.	Διαχειρίζεται τις εκτελέσιμες εφαρμογές		
	β.	Διαχειρίζεται τον αποθηκευτικό χώρο των αρχείων		
	γ.	Συντονίζει τη χρήση των διαφόρων τύπων μνήμης, καταγράφοντας ποια τμήματά τους είναι διαθέσιμα, ποια είναι δεσμευμένα και, αναλόγως με τις απαιτήσεις των διεργασιών, εκχωρεί ή απελευθερώνει τμήματα για να τα χρησιμοποιήσουν οι τελευταίες.		
	δ.	Διαχειρίζεται τις επικοινωνίες με το δίκτυο		
52		Ποιο από τα παρακάτω είναι ένα παράδειγμα φυσικού μέτρου ασφαλείας σε έναν υπολογιστή;		
	α.	Antivirus λογισμικό		
	β.	Χρήση usb-stick για αυθεντικοποίηση		
	γ.	Τοίχος προστασίας (firewall)		
	δ.	Ανακοίνωση αποσύνδεσης (logoff notification)		
53		Ποιο από τα παρακάτω είναι ένα πρότυπο ασφαλείας που περιγράφει πώς πρέπει να αναπτύσσεται, να υλοποιείται και να διατηρείται η ασφάλεια πληροφοριών;		
	α.	ISO 9001		
	β.	IEEE 802.11		
	γ.	ISO 27001		
	δ.	TCP/IP		
54		Τι αποτελεί τον πρώτο παράγοντα ασφάλειας σε ένα φυσικό κτίριο ή εγκατάσταση;		
	α.	Υπολογιστές και δίκτυα		
	β.	Άνθρωποι και πολιτικές ασφαλείας		

	γ.	Κάμερες ασφαλείας		
	δ.	Περιφερειακές συσκευές		
55		Ποιος τύπος κακόβουλου λογισμικού στοχεύει ειδικά στα στοιχεία υλικολογισμικού και υλικού ενός συστήματος υπολογιστή;		
	α.	Ransomware		
	β.	Κατασκοπευτικό λογισμικό		
	γ.	Rootkit		
	δ.	Adware		
56		Ποιος είναι ο πρωταρχικός στόχος των μέτρων ασφαλείας υλικού;		
	α.	Να αποτρέψουν τα τρωτά σημεία του λογισμικού		
	β.	Να προστατεύσουν τα δεδομένα κατά τη μετάδοση		
	γ.	Να προστατεύσουν τα φυσικά εξαρτήματα και περιουσιακά στοιχεία		
	δ.	Να διασφαλίσουν τις διαμορφώσεις του δικτύου		
57		Τι σημαίνει το "SQL" στις επιθέσεις SQL Injection;		
	α.	Structured Query Language		
	β.	Secure Query Link		
	γ.	System Query Logger		
	δ.	Scripted Query Latch		
58		Ποιο από τα παρακάτω ΔΕΝ αποτελεί κοινή απειλή για την ασφάλεια της βάσης δεδομένων;		
	α.	Απειλές εκ των έσω		
	β.	Επιθέσεις Ransomware		
	γ.	Μη εξουσιοδοτημένη πρόσβαση		
	δ.	Κοινωνική μηχανική		

59		Ποιος μηχανισμός ασφάλειας βάσεων δεδομένων περιλαμβάνει τη μετατροπή δεδομένων σε διαφορετική, μη αναστρέψιμη μορφή;		
	α.	Κρυπτογράφηση (Encryption)		
	β.	Hashing μιας διαδρομής (One-way hashing)		
	γ.	Τείχος προστασίας		
	δ.	Σύστημα ανίχνευσης εισβολών (IDS)		
60		Ποιος είναι ο πρωταρχικός σκοπός ενός συστήματος διαχείρισης βάσεων δεδομένων (ΣΔΒΔ) όσον αφορά την ασφάλεια;		
	α.	Να αποτρέψει κάθε μη εξουσιοδοτημένη πρόσβαση στη βάση δεδομένων.		
	β.	Να αποθηκεύει ευαίσθητα δεδομένα σε απλό κείμενο για εύκολη ανάκτηση.		
	γ.	Να διαχειρίζεται και να ελέγχει την πρόσβαση στη βάση δεδομένων.		
	δ.	Να εξαλείφει την ανάγκη για διαδικασίες δημιουργίας αντιγράφων ασφαλείας.		
61		Ποια από τις ακόλουθες δηλώσεις είναι αληθής σχετικά με τα "Zero-Day Exploits";		
	α.	Πρόκειται για ευπάθειες που είναι γνωστές εδώ και πολύ καιρό.		
	β.	Είναι ευπάθειες που αξιοποιούνται μόνο τα Σαββατοκύριακα.		
	γ.	Πρόκειται για ευπάθειες που αξιοποιούνται πριν από τη διάθεση διόρθωσης (patch) του λογισμικού.		
	δ.	Είναι ευπάθειες που επηρεάζουν μόνο λογισμικό zero-day.		
62		Ποια από τις ακόλουθες τεχνικές χρησιμοποιείται συνήθως για την προστασία ευαίσθητων δεδομένων που είναι αποθηκευμένα σε μια βάση δεδομένων;		
	α.	Χρήση αδύναμων κωδικών πρόσβασης		
	β.	Εφαρμογή μηχανισμών ελέγχου πρόσβασης		
	γ.	Αποθήκευση δεδομένων σε απλό κείμενο		
	δ.	Κοινή χρήση των διαπιστευτηρίων της βάσης δεδομένων δημοσίως		

63		Ποιο νομοθετικό κείμενο προστατεύει την ανωνυμία των χρηστών στο Διαδίκτυο;		
	α.	Ο Κανονισμός GDPR της Ευρωπαϊκής Ένωσης.		
	β.	Ο Πολιτικός Κώδικας της Ελλάδας.		
	γ.	Το Ελληνικό Σύνταγμα.		
	δ.	Ο Κώδικας Δικτύου του Διαδικτύου.		
64		Ποιος νόμος παρέχει ασυλία στους παρόχους υπηρεσιών στο Διαδίκτυο για το περιεχόμενο που δημιουργούν οι χρήστες τους;		
	α.	Ο Νόμος για την Ελευθερία της Ενημέρωσης.		
	β.	Ο Κώδικας Δικτύου του Διαδικτύου.		
	γ.	Ο Νόμος για την Πνευματική Ιδιοκτησία.		
	δ.	Το Περί Προστασίας της Προσωπικής Δεδομένης Πληροφορίας.		
65		Ποια από τις παρακάτω πρακτικές αντιβαίνει στον κανόνα του "Net Neutrality";		
	α.	Η προτεραιότητα της διακίνησης περιεχομένου από μεγάλες εταιρίες.		
	β.	Η αυθαίρετη διακοπή της πρόσβασης σε ιστοσελίδες με πολιτικό περιεχόμενο.		
	γ.	Η προσφορά δωρεάν πρόσβασης σε συγκεκριμένες εφαρμογές.		
	δ.	Η ανταγωνιστική τιμολόγηση για την πρόσβαση σε διάφορες ιστοσελίδες.		
66		Ποιο από τα παρακάτω ισχύει ως αντίδραση σε περιπτώσεις διαδικτυακής συκοφαντίας (online defamation);		
	α.	Η διαγραφή όλων των δημοσιεύσεων στον ιστότοπο.		
	β.	Η εκπομπή άμεσης απειλής στον συκοφαντημένο.		
	γ.	Η απαίτηση αποζημίωσης για την υποστηρικτική ανάρτηση ψευδών πληροφοριών.		
	δ.	Η αποκάλυψη της ταυτότητας του συκοφαντούμενου.		
67		Ποιο από τα παρακάτω αποτελεί παράδειγμα παραβίασης της πνευματικής ιδιοκτησίας στο Διαδίκτυο;		

	α.	Κατέβασμα ενός δωρεάν λογισμικού από τον επίσημο ιστότοπο του κατασκευαστή.		
	β.	Αναδημοσίευση ενός άρθρου από έναν ιστοτόπο ειδήσεων με την άδεια του πρωτότυπου εκδότη.		
	γ.	Αναγραφή ενός τραγουδιού στο YouTube χωρίς την άδεια του δημιουργού.		
	δ.	Κοινοποίηση ενός πρωτότυπου λογοτύπου σε ένα blog ως παράδειγμα σχεδίασης.		
68		Τι είναι η έννοια του "Fair Use" στο πλαίσιο του Δικαίου του Διαδικτύου;		
	α.	Η χρήση πνευματικού έργου χωρίς την ανάγκη άδειας ή πληρωμής αποζημίωσης, αν κρίνεται ότι εξυπηρετεί το κοινό συμφέρον.		
	β.	Η προστασία της προσωπικής ιδιοκτησίας σε κάθε περίπτωση, χωρίς εξαιρέσεις.		
	γ.	Η ανακοίνωση δικαιωμάτων πνευματικής ιδιοκτησίας σε έναν διαδικτυακό ιστότοπο.		
	δ.	Η απαίτηση χρηματικής αποζημίωσης για τη χρήση πνευματικού έργου σε διαδικτυακές εφαρμογές.		
69		Ποιος είναι ο πρωταρχικός στόχος της διαχείρισης έργων;		
	α.	Μεγιστοποίηση των κερδών		
	β.	Ελαχιστοποίηση των κινδύνων		
	γ.	Η επίτευξη των στόχων του έργου		
	δ.	Μείωση του εύρους του έργου		
70		Ποιος είναι ο σκοπός του διαγράμματος Gantt στη διαχείριση έργων;		
	α.	Προσδιορισμός των κινδύνων του έργου		
	β.	Κατανομή των πόρων του έργου		
	γ.	Οπτικοποίηση του χρονοδιαγράμματος του έργου		
	δ.	Διαχείριση του προϋπολογισμού του έργου		
71		Ποιος είναι υπεύθυνος για τον εντοπισμό, την αξιολόγηση και τη διαχείριση των κινδύνων καθ' όλη τη διάρκεια του κύκλου ζωής ενός έργου;		
	α.	Διαχειριστής έργου		

	β.	Χορηγός έργου		
	γ.	Stakeholders		
	δ.	Μέλη της ομάδας έργου		
72		Τι αντιπροσωπεύει η κρίσιμη διαδρομή (critical path) σε ένα διάγραμμα δικτύου έργου;		
	α.	Τη μακρύτερη διαδρομή του έργου		
	β.	Η συντομότερη διαδρομή στο έργο		
	γ.	Τη διαδρομή με τους περισσότερους κινδύνους		
	δ.	Η διαδρομή με τους περισσότερους ενδιαφερόμενους		
73		Ποιο από τα παρακάτω δεν αποτελεί παράγοντα του εργασιακού περιβάλλοντος;		
	α.	Η οικονομική κατάσταση της επιχείρησης		
	β.	Η ηλικία του εργατικού δυναμικού		
	γ.	Οι κοινωνικές προσδοκίες		
	δ.	Το χρώμα των τοίχων στο γραφείο		
74		Ποιος παράγοντας δεν επηρεάζει την ικανοποίηση των εργαζομένων στον χώρο εργασίας;		
	α.	Το ύψος του μισθού		
	β.	Η θερμοκρασία στον χώρο εργασίας		
	γ.	Ο αριθμός των ημερών αδείας τους		
	δ.	Η διάρκεια του κινητού τους τηλεφώνου		
75		Ποια είναι η σημασία της πολυπολιτισμικής περιβαλλοντικής ευαισθητοποίησης στον χώρο εργασίας;		
	α.	Να είναι όλοι οι εργαζόμενοι από την ίδια χώρα		
	β.	Να συνεργάζονται όλοι οι εργαζόμενοι στον ίδιο χώρο		
	γ.	Να αντιμετωπίζονται με σεβασμό οι διάφορες πολιτισμικές πρακτικές		
	δ.	Να είναι όλοι οι εργαζόμενοι από την ίδια ηλικιακή ομάδα		

76		Ποιος παράγοντας συμβάλλει στη δημιουργία μιας καλής εργασιακής ηγεσίας;		
	α.	Αυστηρός και απόμακρος διευθυντής		
	β.	Ανεπτυγμένες δεξιότητες επικοινωνίας		
	γ.	Απομόνωση των εργαζομένων από τις αποφάσεις		
	δ.	Ελλείψεις ενθάρρυνσης από τη διοίκηση		
77		Ποιος ορίζεται ως μισθωτός;		
	α.	Κάποιος που διαχειρίζεται τη δική του επιχείρηση		
	β.	Κάποιος που εργάζεται για έναν εργοδότη και λαμβάνει αμοιβή για την εργασία του		
	γ.	Κάποιος που πληρώνει τους εργαζομένους του		
	δ.	Κάποιος που διαχειρίζεται τη δική του ελεύθερη επαγγελματική δραστηριότητα		
78		Ποιο από τα παρακάτω είναι το κύριο χαρακτηριστικό ενός μισθωτού;		
	α.	Ελευθερία στον καθορισμό του ωραρίου εργασίας		
	β.	Ανεξαρτησία από την επιχείρηση ή τον εργοδότη		
	γ.	Αναλογικότητα των εσόδων με τα κέρδη της επιχείρησης		
	δ.	Λήψη αμοιβής σε αντάλλαγμα για την παροχή εργασίας στον εργοδότη		
79		Ποιος είναι ο πρωταρχικός στόχος της ασφάλειας δικτύου;		
	α.	Μεγιστοποίηση της ταχύτητας του δικτύου		
	β.	Ελαχιστοποίηση του κόστους του δικτύου		
	γ.	Προστασία του δικτύου και των επιμέρους στοιχείων του		
	δ.	Επέκταση της εμβέλειας του δικτύου		

80		Τι κάνει ένα τείχος προστασίας στο πλαίσιο της ασφάλειας δικτύου;		
	α.	Προστατεύει από φυσικές εισβολές		
	β.	Φιλτράρει και ελέγχει την κυκλοφορία του δικτύου		
	γ.	Κρυπτογραφεί τα δεδομένα κατά τη μεταφορά		
	δ.	Ενισχύει την απόδοση του δικτύου		
81		Ποιος είναι ο πρωταρχικός σκοπός ενός συστήματος ανίχνευσης εισβολών (IDS);		
	α.	Αποτροπή επιθέσεων		
	β.	Ανίχνευση και ειδοποίηση για ύποπτες δραστηριότητες		
	γ.	Κρυπτογράφηση δεδομένων σε κατάσταση ηρεμίας		
	δ.	Αποκλεισμός κακόβουλων ιστότοπων		
82		Ποιος τύπος κακόβουλου λογισμικού μεταμφιέζεται σε νόμιμο λογισμικό αλλά έχει κακόβουλη πρόθεση;		
	α.	Trojan Horse		
	β.	Worm		
	γ.	Spyware		
	δ.	Ransomware		
83		Τι είναι ένα honeypot στο πλαίσιο της ασφάλειας δικτύων;		
	α.	Ένας τύπος τείχους προστασίας		
	β.	Ένα σύστημα δόλωμα που έχει σχεδιαστεί για να προσελκύει και να παρακολουθεί τους επιτιθέμενους		
	γ.	Μια ασφαλής σήραγγα για τη μετάδοση δεδομένων		
	δ.	Μια μορφή βιομετρικού ελέγχου ταυτότητας		
84		Ποιο από τα παρακάτω ΔΕΝ αποτελεί βέλτιστη πρακτική για την εξασφάλιση συσκευών δικτύου;		
	α.	Να ενημερώνετε τακτικά το υλικολογισμικό και το λογισμικό		

	β.	Απενεργοποιήστε τις περιττές υπηρεσίες και θύρες		
	γ.	Χρησιμοποιήστε προεπιλεγμένους κωδικούς πρόσβασης για εύκολη πρόσβαση		
	δ.	Εφαρμόστε λίστες ελέγχου πρόσβασης (ACL)		
85		Ποιος είναι ο πρωταρχικός σκοπός ενός Εικονικού Ιδιωτικού Δικτύου (VPN);		
	α.	Να κάνει το δίκτυο ταχύτερο		
	β.	Να αποκρύψει τη διεύθυνση IP σας		
	γ.	Να δημιουργήσει μια ασφαλή και ιδιωτική σύνδεση μέσω ενός δημόσιου δικτύου		
	δ.	Να μπλοκάρει τις εισερχόμενες συνδέσεις		
86		Ποιος είναι ο πρωταρχικός στόχος των επιθέσεων κοινωνικής μηχανικής στο πλαίσιο της ασφάλειας δικτύων;		
	α.	Η εκμετάλλευση ευπαθειών λογισμικού		
	β.	Να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συσκευές δικτύου		
	γ.	Να χειραγωγήσουν άτομα ώστε να αποκαλύψουν ευαίσθητες πληροφορίες		
	δ.	Να παραβιάσουν με φυσικό τρόπο την περίμετρο ενός δικτύου		
87		Ποιος είναι ο σκοπός του βρόχου στον προγραμματισμό;		
	α.	Για την προσωρινή αποθήκευση δεδομένων.		
	β.	Για την εκτέλεση μιας συγκεκριμένης εργασίας μία φορά.		
	γ.	Για την επανειλημμένη εκτέλεση ενός συνόλου εντολών.		
	δ.	Για τον ορισμό μιας συνάρτησης.		
88		Ποια από τις ακόλουθες γλώσσες ΔΕΝ είναι γλώσσα προγραμματισμού;		
	α.	Java		
	β.	Go		
	γ.	HTML		

	δ.	PHP		
89		Στον αντικειμενοστραφή προγραμματισμό, ποια είναι η έννοια της ομαδοποίησης των δεδομένων και των μεθόδων που λειτουργούν σε αυτά τα δεδομένα σε μια ενιαία μονάδα;		
	α.	Κλάση		
	β.	Συνάρτηση		
	γ.	Μεταβλητή		
	δ.	Loop		

ΚΑΤΑΛΟΓΟΣ ΕΡΩΤΗΣΕΩΝ ΣΩΣΤΟΥ - ΛΑΘΟΥΣ ΓΙΑ ΤΗΝ ΑΠΟΤΙΜΗΣΗ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ

90		Το firewall χρησιμοποιείται για την κρυπτογράφηση δεδομένων.		
	α.	Σωστό		
	β.	Λάθος		
91		Η διαφοροποίηση των κωδικών πρόσβασης για διάφορες υπηρεσίες αυξάνει την ασφάλεια.		
	α.	Σωστό		
	β.	Λάθος		
92		Το VPN προσφέρει ασφαλή σύνδεση στο Διαδίκτυο και ανωνυμία.		
	α.	Σωστό		
	β.	Λάθος		

93		Η Κοινωνική Μηχανική συνήθως περιλαμβάνει τη χρήση τεχνικών όπως phishing.		
	α.	Σωστό		
	β.	Λάθος		
94		Η αναβάθμιση του λογισμικού σε ένα σύστημα αποτελεί σημαντικό βήμα για την αύξηση της ασφάλειάς του.		
	α.	Σωστό		
	β.	Λάθος		
95		Το Malware είναι γενικά καλό για τα πληροφοριακά συστήματα, καθώς βοηθά στην αναβάθμισή τους.		
	α.	Σωστό		
	β.	Λάθος		
96		Τα σχόλια σε ένα πρόγραμμα προγραμματισμού εκτελούνται κατά τη διάρκεια εκτέλεσης του προγράμματος.		
	α.	Σωστό		
	β.	Λάθος		
97		Οι συναρτήσεις μπορούν να καλούνται μόνο μία φορά σε ένα πρόγραμμα.		
	α.	Σωστό		
	β.	Λάθος		

98		Οι συμβολοσειρές (strings) αναπαριστούν ακέραιους αριθμούς.		
	α.	Σωστό		
	β.	Λάθος		
99		Οι συναρτήσεις στον προγραμματισμό χρησιμοποιούνται για την οργάνωση κώδικα σε μικρότερα τμήματα που μπορούν να επαναχρησιμοποιηθούν.		
	α.	Σωστό		
	β.	Λάθος		
100		Ο τελεστής "&&" στον προγραμματισμό αναπαριστά τον λογικό τελεστή "ή".		
	α.	Σωστό		
	β.	Λάθος		
101		Η κρυπτογραφία είναι η επιστήμη που ασχολείται μόνο με την κρυπτογράφηση των μηνυμάτων.		
	α.	Σωστό		
	β.	Λάθος		
102		Η δημόσια κρυπτογραφία χρησιμοποιεί μόνο ένα κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων.		
	α.	Σωστό		
	β.	Λάθος		

103		Η κρυπτογραφία μπορεί να προστατεύσει μόνο τα δεδομένα που μεταδίδονται μέσω του Διαδικτύου.		
	α.	Σωστό		
	β.	Λάθος		
104		Η κρυπτογραφία είναι μια τεχνική που αποτρέπει την αποκάλυψη των πληροφοριών από μη εξουσιοδοτημένα πρόσωπα.		
	α.	Σωστό		
	β.	Λάθος		
105		Η κρυπτογραφία με δημόσια κλειδιά χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων.		
	α.	Σωστό		
	β.	Λάθος		
106		Η κρυπτογραφία δεν απαιτεί τη χρήση κλειδιών για την προστασία των δεδομένων.		
	α.	Σωστό		
	β.	Λάθος		
107		Το πρωτόκολλο SNMP (Simple Network Management Protocol) χρησιμοποιείται για την ασφαλή απομακρυσμένη διαχείριση δικτύων.		
	α.	Σωστό		
	β.	Λάθος		

108		Οι εξωτερικοί σκληροί δίσκοι είναι παραδείγματα εσωτερικών αποθηκευτικών μέσων.		
	α.	Σωστό		
	β.	Λάθος		
109		Τα δεδομένα στη μνήμη RAM αποθηκεύονται μόνιμα ακόμα και μετά την απενεργοποίηση του υπολογιστή.		
	α.	Σωστό		
	β.	Λάθος		
110		Το Linux είναι ένα λειτουργικό σύστημα, ενώ το Windows είναι μια εφαρμογή.		
	α.	Σωστό		
	β.	Λάθος		
111		Το Linux και το Windows είναι δύο παραδείγματα λειτουργικών συστημάτων.		
	α.	Σωστό		
	β.	Λάθος		
112		Το Windows χρησιμοποιείται σε διάφορες πλατφόρμες, ενώ το Linux είναι διαθέσιμο μόνο για υπολογιστές PC.		
	α.	Σωστό		
	β.	Λάθος		

113		Το Linux χρησιμοποιείται κυρίως σε διακομιστές (servers), ενώ το Windows είναι δημοφιλές για τις επιτραπέζιες χρήσεις.		
	α.	Σωστό		
	β.	Λάθος		
114		Το Linux και το Windows έχουν παρόμοια γραφικά περιβάλλοντα χρήστη.		
	α.	Σωστό		
	β.	Λάθος		
115		Οι επιθέσεις SQL Injection μπορούν να συμβούν μόνο εάν ο κώδικας της εφαρμογής είναι κακογραμμένος και στερείται κατάλληλης επικύρωσης εισόδου.		
	α.	Σωστό		
	β.	Λάθος		
116		Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) περιλαμβάνει τη χρήση πολλαπλών κωδικών πρόσβασης για την πρόσβαση σε ένα σύστημα, ενισχύοντας την ασφάλεια.		
	α.	Σωστό		
	β.	Λάθος		
117		Ο πρωταρχικός σκοπός ενός τείχους προστασίας είναι η κρυπτογράφηση των δεδομένων που είναι αποθηκευμένα σε μια βάση δεδομένων.		
	α.	Σωστό		
	β.	Λάθος		

118		Η πολιτική ασφάλειας πληροφοριακών συστημάτων (cybersecurity policy) αναφέρεται μόνο σε τεχνικά μέτρα και δεν επηρεάζει το Δίκαιο του Διαδικτύου.		
	α.	Σωστό		
	β.	Λάθος		
119		Η Αρχή Προστασίας Δεδομένων είναι υπεύθυνη για την επιβολή των νόμων περί προστασίας της προσωπικής πληροφορίας στην Ευρωπαϊκή Ένωση.		
	α.	Σωστό		
	β.	Λάθος		
120		Ο νόμος περί ιδιωτικής ζωής στο Διαδίκτυο προστατεύει τα πνευματικά δικαιώματα.		
	α.	Σωστό		
	β.	Λάθος		
121		Στη διαχείριση έργων, η κρίσιμη διαδρομή είναι η συντομότερη ακολουθία εργασιών που πρέπει να ολοκληρωθεί για να ολοκληρωθεί ένα έργο.		
	α.	Σωστό		
	β.	Λάθος		
122		Η διαχείριση κινδύνων είναι μια εφάπαξ δραστηριότητα που συνήθως εκτελείται στην αρχή ενός έργου.		
	α.	Σωστό		
	β.	Λάθος		

123		Ένας μισθωτός έχει δικαίωμα σε ελευθερία του λόγου και της έκφρασης στον χώρο εργασίας.		
	α.	Σωστό		
	β.	Λάθος		
124		Κάθε μισθωτός διατηρεί το δικαίωμα να απολαμβάνει ιδιωτικότητα στον χώρο εργασίας.		
	α.	Σωστό		
	β.	Λάθος		
125		Ο μισθωτός έχει δικαίωμα σε ασφαλείς και υγιεινές συνθήκες εργασίας, σύμφωνα με το νόμο.		
	α.	Σωστό		
	β.	Λάθος		
126		Ένα τείχος προστασίας μπορεί να είναι τόσο μια λύση υλικού όσο και μια λύση λογισμικού για την προστασία ενός δικτύου.		
	α.	Σωστό		
	β.	Λάθος		
127		Οι πολιτικές ασφάλειας δικτύου θα πρέπει να επικεντρώνονται μόνο στις εξωτερικές απειλές, καθώς οι εσωτερικές απειλές δεν είναι σημαντικές.		
	α.	Σωστό		
	β.	Λάθος		

128		Η κρυπτογράφηση δεδομένων σε κατάσταση ηρεμίας διασφαλίζει ότι τα δεδομένα προστατεύονται όταν μεταδίδονται ενεργά μέσω ενός δικτύου.		
	α.	Σωστό		
	β.	Λάθος		
129		Ένας ισχυρός και μοναδικός κωδικός πρόσβασης αποτελεί κρίσιμο στοιχείο της ασφάλειας του δικτύου.		
	α.	Σωστό		
	β.	Λάθος		
130		Τα δημόσια δίκτυα Wi-Fi είναι γενικά ασφαλή και δεν απαιτούν πρόσθετες προφυλάξεις.		
	α.	Σωστό		
	β.	Λάθος		
131		Ένα Εικονικό Ιδιωτικό Δίκτυο (VPN) μπορεί να προσφέρει ανωνυμία και απόλυτη ιδιωτικότητα κατά την περιήγηση στο διαδίκτυο.		
	α.	Σωστό		
	β.	Λάθος		
132		Η ασφάλεια υλικού επικεντρώνεται κυρίως στην προστασία του λογισμικού και των δεδομένων από απειλές στον κυβερνοχώρο.		
	α.	Σωστό		
	β.	Λάθος		

133		Τα μέτρα ασφαλείας υλικού, όπως η κρυπτογράφηση υλικού και οι διαδικασίες ασφαλούς εκκίνησης, συμβάλλουν στην προστασία από φυσικές επιθέσεις σε συστήματα υπολογιστών.		
	α.	Σωστό		
	β.	Λάθος		
134		Η ασφάλεια του υλικού είναι αποκλειστικά ευθύνη του τελικού χρήστη και οι οργανισμοί δεν διαδραματίζουν σημαντικό ρόλο στη διασφάλιση της ασφάλειας του υλικού.		
	α.	Σωστό		
	β.	Λάθος		

ΚΑΤΑΛΟΓΟΣ ΕΡΩΤΗΣΕΩΝ ΑΝΤΙΣΤΟΙΧΙΣΗΣ ΓΙΑ ΤΗΝ ΑΠΟΤΙΜΗΣΗ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ

135		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.			
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2		
	α.	Κίνδυνος	1.	Μέτρα που λαμβάνονται για την αντιμετώπιση μιας απειλής σε ένα Πληροφοριακό Σύστημα.	
	β.	Απειλή	2.	Αδυναμίες που μπορεί να υπάρξουν σ' ένα Πληροφοριακό Σύστημα και επιτρέπουν να γίνει κάποια Απειλή πραγματικότητα.	
	γ.	Ευπάθεια	3.	Η πιθανότητα μια απειλή να γίνει πραγματικότητα.	
	δ.	Αντίμετρα ή μέτρα ασφαλείας	4.	Είναι καθετί που μπορεί να συμβεί από ανθρώπινο παράγοντα (πχ. λάθος χειρισμός), φυσικό συμβάν (πχ. πλημμύρα) ή λογισμικό (πχ. Κακόβουλο λογισμικό)	

				και να παρακάμψει κάποια από τις τρεις Βασικές Αρχές: Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα του Πληροφοριακού Συστήματος.		
136		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2			
	α.	Αλγόριθμος	1.	Ένας τρόπος επανάληψης ενός συνόλου εντολών.		
	β.	Μεταβλητή	2.	Μια ακολουθία βημάτων για την επίλυση ενός προβλήματος.		
	γ.	Βρόχος	3.	Μια ονομασμένη θέση αποθήκευσης δεδομένων.		
	δ.	Συνάρτηση	4.	Ένα επαναχρησιμοποιήσιμο τμήμα κώδικα.		
137		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2			
	α.	Python	1.	Γνωστή για την ευελιξία και την αναγνωσιμότητά της.		
	β.	Java	2.	Χρησιμοποιείται συνήθως για την ανάπτυξη ιστοσελίδων.		
	γ.	Javascript	3.	Χρησιμοποιείται για προγραμματισμό σε επίπεδο συστήματος.		
	δ.	C++	4.	Απαιτεί αυστηρή σύνταξη και μεταγλώττιση.		
138		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2			
	α.	Απλή κρυπτογραφία	1.	Κρυπτογραφία με δύο κλειδιά		
	β.	Διπλή κρυπτογραφία	2.	Κρυπτογράφηση με δημόσιο και ιδιωτικό κλειδί		
	γ.	Δημόσια κρυπτογραφία	3.	Κρυπτογραφία με ένα κλειδί		

139	Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2		
	α.	Κρυπτανάλυση	1.	Η διαδικασία κρυπτογράφησης	
	β.	Κρυπτογραφία	2.	Η διαδικασία αποκρυπτογράφησης	
	γ.	Δημόσιο κλειδί	3.	Κλειδί που είναι γνωστό μόνο στον αποδέκτη	
	δ.	Ιδιωτικό κλειδί	4.	Κλειδί που είναι γνωστό σε όλους	
140	Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2		
	α.	Κεντρική μονάδα επεξεργασίας (ΚΜΕ)	1.	Αποθηκεύει μακροπρόθεσμα τα δεδομένα και τα αρχεία του υπολογιστή.	
	β.	Μνήμη RAM	2.	Παρέχει την ικανότητα απεικόνισης γραφικών στην οθόνη του υπολογιστή.	
	γ.	Σκληρός δίσκος (Hard Drive)	3.	Επιτρέπει στον υπολογιστή να εκτελεί εντολές και εφαρμογές.	
	δ.	Κάρτα γραφικών (Graphics Card)	4.	Αποθηκεύει προσωρινά τα δεδομένα κατά τη διάρκεια της λειτουργίας του υπολογιστή.	
141	Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2		
	α.	Ευπάθεια Zero-day	1.	Μια ευπάθεια ασφαλείας που εκμεταλλεύονται οι επιτιθέμενοι πριν από τη διάθεση ενός patch (διόρθωσης) στο λογισμικό του συστήματος.	
	β.	Διαχείριση διορθώσεων (Patch management)	2.	Η διαδικασία τακτικής ενημέρωσης και εφαρμογής διορθώσεων ασφαλείας σε λογισμικό και συστήματα.	

	γ.	Κοινωνική μηχανική	3.	Η χειραγώγηση ατόμων ώστε να αποκαλύψουν εμπιστευτικές πληροφορίες ή να εκτελέσουν ενέργειες που θέτουν σε κίνδυνο την ασφάλεια.		
142		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
		ΣΤΗΛΗ 1		ΣΤΗΛΗ 2		
	α.	GDPR	1.	Επίθεση που στοχεύει την υπερφόρτωση των δικτυακών πόρων.		
	β.	DDOS	2.	Κανονισμός περί προστασίας δεδομένων πολιτών της ΕΕ.		
	γ.	Πνευματική Ιδιοκτησία	3.	Νόμος περί ανεπιθύμητης αλληλογραφίας στο ηλεκτρονικό ταχυδρομείο.		
	δ.	Νόμος CAN-SPAM	4.	Προστασία πνευματικών δικαιωμάτων για δημιουργίες στο Διαδίκτυο.		
143		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
		ΣΤΗΛΗ 1		ΣΤΗΛΗ 2		
	α.	Κλείσιμο	1.	Καθορισμός του πεδίου εφαρμογής του έργου, των στόχων και δημιουργία ενός χάρτη έργου.		
	β.	Έναρξη	2.	Ολοκλήρωση όλων των δραστηριοτήτων του έργου και εξασφάλιση της ολοκλήρωσης όλων των παραδοτέων.		
	γ.	Εκτέλεση	3.	Εκτέλεση των εργασιών του έργου σύμφωνα με το σχέδιο έργου.		
	δ.	Παρακολούθηση και έλεγχος	4.	Τακτική παρακολούθηση και μέτρηση της απόδοσης του έργου.		
144		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
		ΣΤΗΛΗ 1		ΣΤΗΛΗ 2		

	α.	Δικαίωμα στην ισότιμη αμοιβή	1.	Το δικαίωμα των εργαζομένων να λαμβάνουν ίση αμοιβή για ίση εργασία χωρίς διακρίσεις.		
	β.	Δικαίωμα στην ασφαλή εργασιακή περιβαλλοντική ατμόσφαιρα	2.	Το δικαίωμα των εργαζομένων να εργάζονται σε περιβάλλον χωρίς κίνδυνο για την υγεία και την ασφάλειά τους.		
	γ.	Δικαίωμα στην ελευθερία του συνδικαλισμού	3.	Το δικαίωμα των εργαζομένων να συμμετέχουν σε συνδικαλιστικές οργανώσεις και δραστηριότητες χωρίς αναστολές ή διώξεις.		
145	Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.					
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2			
	α.	Firewall	1.	Ένας τύπος επίθεσης στον κυβερνοχώρο όπου οι επιτιθέμενοι εξαπατούν τα άτομα ώστε να αποκαλύψουν ευαίσθητες πληροφορίες, όπως διαπιστευτήρια σύνδεσης, παριστάνοντας μια αξιόπιστη οντότητα.		
	β.	Phishing	2.	Ένα σύστημα ασφαλείας που παρακολουθεί την κυκλοφορία του δικτύου για ύποπτες δραστηριότητες ή μοτίβα και παράγει ειδοποιήσεις ή αναλαμβάνει δράση όταν εντοπίζονται πιθανές απειλές.		
	γ.	Σύστημα ανίχνευσης εισβολής (IDS)	3.	Η διαδικασία μετατροπής δεδομένων σε ασφαλή μορφή για την προστασία τους από μη εξουσιοδοτημένη πρόσβαση, διασφαλίζοντας ότι μόνο εξουσιοδοτημένα μέρη μπορούν να αποκρυπτογραφήσουν και να αποκτήσουν πρόσβαση		

				στις πληροφορίες.		
	δ.	Κρυπτογράφηση	4.	Ένα σύστημα ασφαλείας βασισμένο σε λογισμικό ή υλικό που παρακολουθεί και ελέγχει την εισερχόμενη και εξερχόμενη κυκλοφορία δικτύου με βάση προκαθορισμένους κανόνες ασφαλείας.		
146	Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.					
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2			
	α.	VPN	1.	Ελέγξτε και διαχειριστείτε την πρόσβαση στο δίκτυο, καθορίζοντας ποιοι χρήστες ή συσκευές επιτρέπεται ή απαγορεύεται να έχουν πρόσβαση σε συγκεκριμένους πόρους.		
	β.	Βιομετρική αυθεντικοποίηση	2.	Ανίχνευση και αφαίρεση ή απομόνωση κακόβουλου λογισμικού, όπως ιοί και κακόβουλο λογισμικό, για την προστασία των συστημάτων από μολύνσεις.		
	γ.	Λογισμικού antivirus	3.	Επαλήθευση της ταυτότητας των χρηστών βάσει μοναδικών φυσικών χαρακτηριστικών ή χαρακτηριστικών συμπεριφοράς, όπως δακτυλικά αποτυπώματα ή αναγνώριση προσώπου.		
	δ.	Λίστες ελέγχου πρόσβασης (ACL)	4.	Δημιουργία ασφαλούς και κρυπτογραφημένης σύνδεσης μέσω ενός μη αξιόπιστου δικτύου, όπως το διαδίκτυο, για την προστασία των δεδομένων κατά τη μετάδοση.		

147	Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2		
	α.	Αναγνώριση (Reconnaissance)	1.	Μετά την επιτυχή εκμετάλλευση μιας ευπάθειας, ο ελεγκτής μπορεί να εκτελέσει πρόσθετες ενέργειες, όπως κλιμάκωση προνομίων ή διαρροή δεδομένων, για να εκτιμήσει τον αντίκτυπο μιας παραβίασης.	
	β.	Εκμετάλλευση (Exploitation)	2.	Σε αυτή τη φάση, ο ελεγκτής συλλέγει πληροφορίες σχετικά με το σύστημα ή το δίκτυο-στόχο, όπως διευθύνσεις IP, ονόματα τομέων και πιθανές ευπάθειες.	
	γ.	Αναφορά (Reporting)	3.	Κατά τη διάρκεια αυτής της φάσης, ο ελεγκτής προσπαθεί να εκμεταλλευτεί τα εντοπισμένα τρωτά σημεία για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση ή έλεγχο στο σύστημα-στόχο.	
148	δ.	Μετά την εκμετάλλευση (Post-Exploitation)	4.	Στη φάση της αναφοράς, ο ελεγκτής τεκμηριώνει τα ευρήματα, τα τρωτά σημεία και τα συνιστώμενα βήματα αποκατάστασης για να τα παρουσιάσει στον πελάτη ή τον οργανισμό.	
	Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2		
148	α.	Trusted Platform Module (TPM)	1.	Μια ειδική συσκευή υλικού για κρυπτογραφικές λειτουργίες και διαχείριση κλειδιών.	
	β.	Hardware Security Module (HSM)	2.	Εξασφαλίζει ότι μόνο ψηφιακά υπογεγραμμένο και αξιόπιστο λογισμικό μπορεί να εκτελεστεί κατά τη διαδικασία εκκίνησης.	

	γ.	Secure Boot	3.	Ένα στοιχείο υλικού που αποθηκεύει κλειδιά κρυπτογράφησης και παρέχει ασφαλή αποθήκευση και κρυπτογραφικές λειτουργίες.		
149		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
		ΣΤΗΛΗ 1	ΣΤΗΛΗ 2			
	α.	Βιομετρική πιστοποίηση ταυτότητας	1.	Μηχανισμοί ασφαλείας που χρησιμοποιούν φυσικά χαρακτηριστικά, όπως δακτυλικά αποτυπώματα ή σαρώσεις αμφιβληστροειδούς, για τον έλεγχο ταυτότητας του χρήστη.		
	β.	Σφραγίδες ασφαλείας για παραβίαση (Tamper-Evident Seals)	2.	Φυσικά μέτρα ασφαλείας που αποκαλύπτουν προσπάθειες παραποίησης με σπάσιμο ή αλλοίωση σφραγίδων.		
	γ.	Κλειδαριές καλωδίων	3.	Συσκευές ή μηχανισμοί που χρησιμοποιούνται για τη φυσική ασφάλεια του εξοπλισμού υπολογιστών για την αποτροπή κλοπής.		
150		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
		ΣΤΗΛΗ 1	ΣΤΗΛΗ 2			
	α.	Hardware Network Firewall	1.	Παρακολουθεί την κυκλοφορία του δικτύου και επιβάλλει πολιτικές ελέγχου πρόσβασης για την προστασία από μη εξουσιοδοτημένη πρόσβαση και επιθέσεις.		
	β.	Intrusion Detection System (IDS)	2.	Συσκευή που παράγει κωδικούς πρόσβασης μίας χρήσης για έλεγχο		

				ταυτότητας δύο παραγόντων.		
	γ.	Hardware Security Token	3.	Ανιχνεύει και ειδοποιεί για πιθανές παραβιάσεις ασφαλείας ή προσπάθειες μη εξουσιοδοτημένης πρόσβασης σε ένα δίκτυο ή σύστημα.		

3. ΕΡΩΤΗΣΕΙΣ ΠΡΑΚΤΙΚΗΣ ΚΑΤΕΥΘΥΝΣΗΣ

ΚΑΤΑΛΟΓΟΣ ΕΡΩΤΗΣΕΩΝ ΠΟΛΛΑΠΛΗΣ ΕΠΙΛΟΓΗΣ ΓΙΑ ΤΗΝ ΑΠΟΤΙΜΗΣΗ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ

1		# Υποθέτουμε τον παρακάτω κώδικα Python: <pre>num1 = 10 num2 = 5 result = num1 + num2 if result > 15: print("Το αποτέλεσμα είναι μεγαλύτερο από 15.") elif result < 10: print("Το αποτέλεσμα είναι μικρότερο από 10.") else: print("Το αποτέλεσμα είναι μεταξύ 10 και 15.")</pre> Τι τιμή έχει η μεταβλητή result μετά την εκτέλεση του κώδικα;				
	α.	5				
	β.	10				
	γ.	15				
	δ.	20				

2		# Υποθέτουμε τον παρακάτω κώδικα Python: <pre> num1 = 10 num2 = 5 result = num1 + num2 if result > 15: print("Το αποτέλεσμα είναι μεγαλύτερο από 15.") elif result < 10: print("Το αποτέλεσμα είναι μικρότερο από 10.") else: print("Το αποτέλεσμα είναι μεταξύ 10 και 15.") </pre> Τι θα εμφανιστεί στην οθόνη αν η συνθήκη εκπληρωθεί με βάση την τιμή του προηγούμενου ερωτήματος;		
	α.	Το αποτέλεσμα είναι μικρότερο από 10.		
	β.	Το αποτέλεσμα είναι μεγαλύτερο από 15.		
	γ.	Το αποτέλεσμα είναι μεταξύ 10 και 15.		
	δ.	Κενό μήνυμα.		
3		Ποιος αλγόριθμος κρυπτογραφίας χρησιμοποιείται συνήθως για την ασφαλή περιήγηση στο διαδίκτυο;		
	α.	DES (Data Encryption Standard)		
	β.	RSA (Rivest-Shamir-Adleman)		
	γ.	SSL/TLS (Secure Sockets Layer/Transport Layer Security)		
	δ.	MD5 (Message Digest Algorithm 5)		
4		Ποιο από τα παρακάτω αποτελεί ένα από τα βασικά χαρακτηριστικά των κρυπτογραφικών κλειδιών;		
	α.	Είναι δημόσια γνωστά.		
	β.	Είναι πολύ απλά και ευανάγνωστα.		
	γ.	Πρέπει να είναι μακρά και πολύπλοκα.		
	δ.	Πρέπει να διατηρούνται μυστικά και να είναι αρκετά ασφαλή		
5		Ποιο από τα παρακάτω είναι ένα παράδειγμα κρυπτογραφικού αλγορίθμου που χρησιμοποιείται για την ψηφιακή υπογραφή;		

	α.	AES (Advanced Encryption Standard)		
	β.	DES (Data Encryption Standard)		
	γ.	RSA (Rivest-Shamir-Adleman)		
	δ.	SHA-256 (Secure Hash Algorithm 256-bit)		
6		Ένας αποστολέας θέλει να στείλει ένα μυστικό μήνυμα σε έναν παραλήπτη χρησιμοποιώντας δημόσια κλειδιά. Ποια από τις παρακάτω επιλογές είναι η σωστή διαδικασία για να επιτευχθεί αυτό;		
	α.	Ο αποστολέας κρυπτογραφεί το μήνυμά του με το δημόσιο κλειδί του παραλήπτη και στέλνει το κρυπτογραφημένο μήνυμα.		
	β.	Ο αποστολέας κρυπτογραφεί το μήνυμά του με το ιδιωτικό κλειδί του παραλήπτη και στέλνει το κρυπτογραφημένο μήνυμα.		
	γ.	Ο αποστολέας κρυπτογραφεί το μήνυμά του με το ιδιωτικό κλειδί του και στέλνει το κρυπτογραφημένο μήνυμα.		
	δ.	Ο αποστολέας δεν μπορεί να χρησιμοποιήσει δημόσια κλειδιά για να στείλει μυστικά μηνύματα.		
7		Ποιο από τα παρακάτω είναι παράδειγμα κρυπτογραφικού πρωτοκόλλου για ασφαλή επικοινωνία στο Διαδίκτυο;		
	α.	HTTP		
	β.	FTP		
	γ.	SSH		
	δ.	SMTP		
8		Ποιο από τα παρακάτω είναι ένα πρωτόκολλο ασφαλούς επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου;		
	α.	FTP		
	β.	SMTP		
	γ.	HTTP		
	δ.	Telnet		
9		Ποιο από τα παρακάτω είναι ένα παράδειγμα λειτουργικού συστήματος ανοιχτού κώδικα για ηλεκτρονικό υπολογιστή;		

	α.	Windows		
	β.	macOS		
	γ.	Linux		
	δ.	Android		
10		Ποιο από τα παρακάτω είναι ένα σύστημα αρχείων που χρησιμοποιείται συνήθως σε λειτουργικά συστήματα τύπου Unix/Linux;		
	α.	NTFS		
	β.	FAT32		
	γ.	Ext4		
	δ.	HFS+		
11		Ποια από τις παρακάτω είναι εντολή που χρησιμοποιείται στο Linux για να δημιουργήσετε έναν νέο κατάλογο (φάκελο);		
	α.	mkdir		
	β.	create folder		
	γ.	new directory		
	δ.	mkfolder		
12		Ποια εντολή χρησιμοποιείται στα Windows για να εμφανίσετε τον κατάλογο (φάκελο) ενός τρέχοντος φακέλου;		
	α.	list		
	β.	dir		
	γ.	show folder		
	δ.	display directory		
13		Ποιο από τα ακόλουθα ΔΕΝ αποτελεί κοινό φορέα επίθεσης για την ασφάλεια λογισμικού και βάσεων δεδομένων;		
	α.	Έγχυση SQL		
	β.	Cross-Site Scripting (XSS)		
	γ.	Επίθεση τύπου Denial of service (DDoS)		

	δ.	Secure Sockets Layer (SSL)		
14		Ποιος τύπος κρυπτογράφησης χρησιμοποιείται συνήθως για την ασφάλεια των δεδομένων σε κατάσταση ηρεμίας σε μια βάση δεδομένων;		
	α.	Συμμετρική κρυπτογράφηση		
	β.	Ασύμμετρη κρυπτογράφηση		
	γ.	Κρυπτογράφηση		
	δ.	Salting		
15		Ποιο από τα ακόλουθα αποτελεί παράδειγμα ισχυρής πολιτικής κωδικού πρόσβασης;		
	α.	Ο κωδικός πρόσβασης πρέπει να έχει μήκος τουλάχιστον 6 χαρακτήρων.		
	β.	Ένας κωδικός πρόσβασης πρέπει να περιέχει τουλάχιστον ένα κεφαλαίο γράμμα.		
	γ.	Ένας κωδικός πρόσβασης πρέπει να αλλάζει κάθε 30 ημέρες.		
	δ.	Ένας κωδικός πρόσβασης πρέπει να είναι μια κοινή λέξη λεξικού.		
16		Ποιο από τα παρακάτω ΔΕΝ αποτελεί κοινό μέτρο ασφαλείας για την προστασία από επιθέσεις Cross-Site Scripting (XSS);		
	α.	Επικύρωση εισόδου (Input validation)		
	β.	Κωδικοποίηση εξόδου (Output encoding)		
	γ.	Διαχείριση συνεδρίας (Session management)		
	δ.	Κρυπτογράφηση βάσης δεδομένων (Database encryption)		
17		Ποιος είναι ο όρος για μια ευπάθεια ασφαλείας που εμφανίζεται όταν μια εφαρμογή δεν επικυρώνει ή δεν καθαρίζει σωστά τα δεδομένα εισόδου του χρήστη, επιτρέποντας την εκτέλεση κακόβουλων δεδομένων εισόδου ως κώδικα;		
	α.	Υπερχείλιση προσωρινής μνήμης		
	β.	Cross-Site Scripting (XSS)		
	γ.	Ευπάθεια IDOR (Insecure Direct Object Reference)		
	δ.	Zero-day exploit		

18		Ποιος είναι ο κύριος σκοπός ενός τείχους προστασίας εφαρμογών ιστού (WAF) στο πλαίσιο της ασφάλειας λογισμικού και βάσεων δεδομένων;		
	α.	Να διασφαλίσει το φυσικό υλικό των διακομιστών ιστού		
	β.	Να προστατεύει από επιθέσεις που βασίζονται στον ιστό και να φιλτράρει την εισερχόμενη κυκλοφορία (incoming traffic filtering)		
	γ.	Να παρέχει έλεγχο ταυτότητας για τους χρήστες που έχουν πρόσβαση σε εφαρμογές ιστού		
	δ.	Για τη βελτιστοποίηση της απόδοσης των εφαρμογών ιστού		
19		Ποιο έγγραφο περιγράφει το πεδίο εφαρμογής, τους στόχους και τα παραδοτέα του έργου, χρησιμεύοντας ως οδηγός καθ' όλη τη διάρκεια του κύκλου ζωής του έργου;		
	α.	Χάρτης έργου (project charter)		
	β.	Διάγραμμα Gantt		
	γ.	Καταγραφή κινδύνων		
	δ.	Ανάλυση των ενδιαφερομένων μερών (stakeholder analysis)		
20		Ποια μεθοδολογία διαχείρισης έργων δίνει έμφαση στην ευελιξία, την προσαρμοστικότητα και τη συνεχή βελτίωση;		
	α.	Waterfall		
	β.	Agile		
	γ.	Six Sigma		
	δ.	Prince2		
21		Ποιο από τα ακόλουθα είναι μια κοινή επίθεση ασφάλειας δικτύου που περιλαμβάνει την υποκλοπή και την τροποποίηση της επικοινωνίας μεταξύ δύο μερών;		
	α.	Phishing		
	β.	DDoS		
	γ.	Man-in-the-Middle (MitM)		
	δ.	SQL Injection		

22		Ποιο πρωτόκολλο κρυπτογράφησης χρησιμοποιείται συνήθως για την ασφάλεια των δεδομένων που μεταδίδονται μέσω του διαδικτύου, ιδίως για ιστότοπους (HTTPS);		
	α.	DES		
	β.	WEP		
	γ.	SSL/TLS		
	δ.	IPsec		
23		Ποιο πρωτόκολλο ασφαλείας χρησιμοποιείται για τη δημιουργία ασφαλούς απομακρυσμένης σύνδεσης σε ένα δίκτυο μέσω ενός μη αξιόπιστου δικτύου, όπως το διαδίκτυο;		
	α.	HTTP		
	β.	SSH		
	γ.	SMTP		
	δ.	SNMP		
24		Ποια είναι μια κοινή μέθοδος προστασίας ενός ασύρματου δικτύου από μη εξουσιοδοτημένη πρόσβαση;		
	α.	Απενεργοποίηση της κρυπτογράφησης		
	β.	Χρήση WEP		
	γ.	Εφαρμογή ισχυρής κρυπτογράφησης WPA/WPA2		
	δ.	Εκπομπή του SSID		
25		Ποιο μέτρο ασφαλείας μπορεί να προστατεύσει από επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DDoS);		
	α.	Λογισμικό προστασίας από ιούς		
	β.	Σύστημα πρόληψης εισβολών (IPS)		
	γ.	Ισχυρές πολιτικές κωδικών πρόσβασης		
	δ.	Περιορισμός του ρυθμού και φιλτράρισμα της κυκλοφορίας		
26		Ποια είναι μια κοινή μέθοδος πιστοποίησης χρηστών σε ένα δίκτυο με βάση τα μοναδικά φυσικά χαρακτηριστικά τους, όπως δακτυλικά αποτυπώματα ή σαρώσεις		

		αμφιβληστροειδούς;		
	α.	Έλεγχος ταυτότητας με token		
	β.	Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA)		
	γ.	Βιομετρικός έλεγχος ταυτότητας		
	δ.	Πιστοποίηση ταυτότητας βάσει πιστοποιητικού		
27		Ποια είναι η πρώτη γραμμή άμυνας κατά του κακόβουλου λογισμικού στην ασφάλεια δικτύου;		
	α.	Σύστημα ανίχνευσης εισβολών (IDS)		
	β.	Τείχος προστασίας		
	γ.	Λογισμικό προστασίας από ιούς		
	δ.	Κρυπτογράφηση		
28		Ποιο είδος επίθεσης περιλαμβάνει την πλημμύρα ενός δικτύου ή ενός ιστότοπου με υπερβολικό όγκο κίνησης για τη διακοπή της κανονικής λειτουργίας του;		
	α.	Phishing		
	β.	Man-in-the-Middle (MitM)		
	γ.	Distributed Denial of Service (DDoS)		
	δ.	SQL Injection		
29		Ποια τεχνολογία ασφάλειας δικτύου κρυπτογραφεί τα δεδομένα στον αποθηκευτικό χώρο μιας συσκευής για να αποτρέψει τη μη εξουσιοδοτημένη πρόσβαση σε περίπτωση κλοπής ή απώλειας;		
	α.	Τείχος προστασίας		
	β.	VPN		
	γ.	BitLocker		
	δ.	DNSSEC		
30		Ποιο πρωτόκολλο χρησιμοποιείται συνήθως για ασφαλή επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου;		
	α.	HTTP		

	β.	IMAP		
	γ.	SMTP		
	δ.	POP3		

ΚΑΤΑΛΟΓΟΣ ΕΡΩΤΗΣΕΩΝ ΠΟΛΛΑΠΛΗΣ ΕΠΙΛΟΓΗΣ ΓΙΑ ΤΗΝ ΑΠΟΤΙΜΗΣΗ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ

31		Ο Έλεγχος Πρόσβασης (Access control) εφαρμόζεται σε 3 περιπτώσεις: Δικτυακή Πρόσβαση, Πρόσβαση σε συστήματα, Πρόσβαση στα δεδομένα.		
	α.	Σωστό		
	β.	Λάθος		
32		Ο τελεστής "==" χρησιμοποιείται για τον έλεγχο ισότητας μεταξύ δύο τιμών.		
	α.	Σωστό		
	β.	Λάθος		
33		Η ασύμμετρη κρυπτογραφία χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων.		
	α.	Σωστό		
	β.	Λάθος		
34		Η επίθεση DDoS (Distributed Denial of Service) είναι ένας τύπος επίθεσης που στοχεύει στην εξανάγκαση ενός δικτύου ή ιστοτόπου να γίνει προσβάσιμος από ανεπιθύμητη κυκλοφορία.		
	α.	Σωστό		
	β.	Λάθος		

35		Το Linux δεν είναι ανοιχτού κώδικα και το Windows δεν είναι προστατευμένο από πνευματικά δικαιώματα.		
	α.	Σωστό		
	β.	Λάθος		
36		Μια ισχυρή πολιτική κωδικών πρόσβασης απαιτεί από τους χρήστες να μοιράζονται τους κωδικούς πρόσβασής τους με τους συναδέλφους τους, ώστε να διασφαλίζεται η προσβασιμότητα.		
	α.	Σωστό		
	β.	Λάθος		
37		Η agile διαχείριση έργων είναι μια προσέγγιση που δεν επιτρέπει αλλαγές μόλις ξεκινήσει το έργο.		
	α.	Σωστό		
	β.	Λάθος		
38		Ο έλεγχος ταυτότητας δύο παραγόντων (2FA) περιλαμβάνει τη χρήση δύο διαφορετικών παραγόντων ελέγχου ταυτότητας από την ίδια κατηγορία.		
	α.	Σωστό		
	β.	Λάθος		
39		Στο Linux, η εντολή "cd" χρησιμοποιείται για την αλλαγή καταλόγων, ενώ στα Windows, η αντίστοιχη εντολή είναι "chdir".		
	α.	Σωστό		
	β.	Λάθος		

40		Η εντολή "pwd" χρησιμοποιείται για την εκτύπωση του καταλόγου εργασίας τόσο στα κελύφη εντολών του Linux όσο και στα κελύφη εντολών των Windows.		
	α.	Σωστό		
	β.	Λάθος		
41		Στα Windows, η εντολή "ipconfig" χρησιμοποιείται για την εμφάνιση πληροφοριών διαμόρφωσης δικτύου, ενώ στο Linux, η αντίστοιχη εντολή είναι η "ifconfig".		
	α.	Σωστό		
	β.	Λάθος		

ΚΑΤΑΛΟΓΟΣ ΕΡΩΤΗΣΕΩΝ ΑΝΤΙΣΤΟΙΧΙΣΗΣ ΓΙΑ ΤΗΝ ΑΠΟΤΙΜΗΣΗ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ

42		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.		
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2	
	α.	Εμπιστευτικότητα	1. Εξασφαλίζει πως τα δεδομένα δε θα υποστούν καμία αλλοίωση από μη εξουσιοδοτημένα άτομα ή με μη ανιχνεύσιμο τρόπο.	
	β.	Διαθεσιμότητα	2. Η εξασφάλιση πως τα δεδομένα δε θα γίνουν διαθέσιμα, δε θα μπορούν να τα διαβάσουν δηλαδή, μη εξουσιοδοτημένα άτομα.	
	γ.	Ακεραιότητα	3. Εξασφαλίζει πως το σύστημα θα μπορεί να παρέχει τις πληροφορίες του, όταν του ζητηθούν και μέσα σε αποδεκτά χρονικά όρια.	
43		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.		

	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2			
	α.	Integer	1.	Αναπαράσταση συμβολοσειρών		
	β.	String	2.	Αποθήκευση ακεραίων αριθμών		
	γ.	Boolean	3.	Αποθήκευση αριθμών με υποδιαστολή		
	δ.	Float	4.	Αναπαράσταση true-false		
44	Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.					
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2			
	α.	If-else	1.	Χρησιμοποιείται για αποφάσεις που στηρίζονται σε συνθήκες		
	β.	For loop	2.	Χρησιμοποιείται για επανάληψη κώδικα πεπερασμένες φορές		
	γ.	Switch-case-default	3.	Χρησιμοποιείται για επανάληψη κώδικα όσο ισχύει ή συνθήκη		
	δ.	While-do	4.	Χρησιμοποιείται για τη δημιουργία πολλαπλών συνθηκών με μία γενική συνθήκη στο τέλος		
45	Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.					
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2			
	α.	Κρυπτογραφικός αλγόριθμος	1.	Κρυπτογραφία με ένα κλειδί		
	β.	Συμμετρική κρυπτογραφία	2.	Μαθηματική διαδικασία για την κρυπτογράφηση και αποκρυπτογράφηση		
	γ.	Ασύμμετρη κρυπτογραφία	3.	Παράμετρος που χρησιμοποιείται στον αλγόριθμο		
	δ.	Κλειδί	4.	Κρυπτογραφία με δύο κλειδιά		

46		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.			
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2		
	α.	VPN (Virtual Private Network)	1.	Πρωτόκολλο ασφαλούς επικοινωνίας για ιστοσελίδες	
	β.	IDS (Intrusion Detection System)	2.	Σύστημα που εντοπίζει ανεπιθύμητες εισβολές σε ένα δίκτυο	
	γ.	Firewall	3.	Τεχνολογία που δημιουργεί ασφαλή σύνδεση μεταξύ δικτύων	
	δ.	SSL/TLS	4.	Ένα είδος φραγής πρόσβασης σε ένα δίκτυο	
47		Ταιριάζτε το καθένα από τα παρακάτω χαρακτηριστικά με το σωστό λειτουργικό σύστημα, Windows ή Linux.			
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2		
	α.	Χρήση του NTFS συστήματος αρχείων.	1.	Windows	
	β.	Εντολές του κέλυφους (shell commands) περιλαμβάνουν την εντολή "ls".	2.	Linux	
	γ.	Το λειτουργικό σύστημα είναι ανοιχτού κώδικα.			
	δ.	Ο Internet Explorer είναι ο προεπιλεγμένος περιηγητής ιστού.			
48		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.			
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2		
	α.	Cross-Site Scripting (XSS)	1.	Ένας τύπος επίθεσης όπου ένας επιτιθέμενος εισάγει	

				κακόβουλα σενάρια σε εφαρμογές ιστού τα οποία στη συνέχεια εκτελούνται από άλλους χρήστες.		
	β.	Έλεγχος ταυτότητας δύο παραγόντων (2FA)	2.	Ένα μέτρο ασφαλείας που απαιτεί από τους χρήστες να παρέχουν δύο διαφορετικούς παράγοντες ελέγχου ταυτότητας για την πρόσβαση σε ένα σύστημα ή μια εφαρμογή.		
	γ.	Επικάλυψη δεδομένων (Data masking)	3.	Η πρακτική της απόκρυψης των αρχικών δεδομένων με τροποποιημένο περιεχόμενο για την προστασία ευαίσθητων		
49		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2			
	α.	Σύστημα πρόληψης εισβολών (Intrusion Prevention System)	1.	Εντοπισμός και αποκλεισμός ύποπτης κυκλοφορίας δικτύου σε πραγματικό χρόνο.		
	β.	Secure Socket Layer (SSL)	2.	Κρυπτογράφηση των δεδομένων που μεταδίδονται μεταξύ του προγράμματος περιήγησης ενός χρήστη και ενός διακομιστή ιστού για ασφαλή επικοινωνία.		
	γ.	Τείχος προστασίας βάσεων δεδομένων	3.	Παρακολούθηση και αποτροπή μη εξουσιοδοτημένης πρόσβασης σε μια βάση δεδομένων.		
50		Αντιστοιχίστε τις ακόλουθες έννοιες της στήλης 1 με τη στήλη 2.				
	ΣΤΗΛΗ 1		ΣΤΗΛΗ 2			
	α.	Malware	1.	Κακόβουλο λογισμικό που έχει σχεδιαστεί για να θέσει σε κίνδυνο, να βλάψει ή να κλέψει δεδομένα από έναν υπολογιστή ή ένα δίκτυο.		
	β.	Phishing	2.	Ένας τύπος επίθεσης κοινωνικής μηχανικής όπου οι επιτιθέμενοι χρησιμοποιούν παραπλανητικά μηνύματα		

			ηλεκτρονικού ταχυδρομείου ή μηνύματα για να εξαπατήσουν τα άτομα.		
γ.	SQL Injection	3.	Κυβερνοεπίθεση κατά την οποία ένας εισβολέας εκμεταλλεύεται την έλλειψη ελέγχου των δεδομένων εισόδου σε μια εφαρμογή, ώστε να εισαγάγει κακόβουλες εντολές σε πεδία που περιμένουν κανονικά δεδομένα.		
δ.	Ευπάθεια Zero-day	4.	Άγνωστη και ανεπίλυτη ευπάθεια σε λογισμικό, για την οποία ο κατασκευαστής δεν έχει κυκλοφορήσει ακόμη ενημέρωση (patch), δίνοντας στους κακόβουλους χρήστες χρόνο να την εκμεταλλευτούν πριν γίνει γνωστή και αντιμετωπιστεί.		

4. ΑΠΑΝΤΗΣΕΙΣ ΘΕΩΡΗΤΙΚΗΣ ΚΑΤΕΥΘΥΝΣΗΣ

ΚΑΤΑΛΟΓΟΣ ΑΠΑΝΤΗΣΕΩΝ ΣΤΙΣ ΕΡΩΤΗΣΕΙΣ ΠΟΛΛΑΠΛΗΣ ΕΠΙΛΟΓΗΣ ΓΙΑ ΤΗΝ ΑΠΟΤΙΜΗΣΗ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ	
A/A Ερώτησης	Σωστή απάντηση
1	γ
2	γ
3	β
4	γ
5	β
6	γ
7	γ
8	β
9	δ
10	γ
11	α
12	β
13	γ
14	γ
15	α

16	β
17	β
18	β
19	γ
20	β
21	β
22	β
23	γ
24	γ
25	γ
26	γ
27	β
28	β
29	α
30	γ
31	δ
32	α
33	γ
34	β
35	γ
36	α
37	γ
38	β
39	γ
40	γ
41	γ
42	γ
43	γ
44	γ
45	α
46	γ
47	δ
48	γ
49	δ
50	δ
51	γ
52	β
53	γ
54	β

55	γ
56	γ
57	α
58	β
59	β
60	γ
61	γ
62	β
63	α
64	α
65	α
66	γ
67	γ
68	α
69	γ
70	γ
71	α
72	α
73	δ
74	δ
75	γ
76	β
77	β
78	δ
79	γ
80	β
81	β
82	α
83	β
84	γ
85	γ
86	γ
87	γ
88	γ
89	α
ΚΑΤΑΛΟΓΟΣ ΑΠΑΝΤΗΣΕΩΝ ΣΤΙΣ ΕΡΩΤΗΣΕΙΣ ΣΩΣΤΟΥ - ΛΑΘΟΥΣ ΓΙΑ ΤΗΝ ΑΠΟΤΙΜΗΣΗ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ	
A/A Ερώτησης	Σωστή απάντηση

90	Λάθος
91	Σωστό
92	Σωστό
93	Σωστό
94	Σωστό
95	Λάθος
96	Λάθος
97	Λάθος
98	Λάθος
99	Σωστό
100	Λάθος
101	Λάθος
102	Λάθος
103	Λάθος
104	Σωστό
105	Λάθος
106	Λάθος
107	Σωστό
108	Λάθος
109	Λάθος
110	Λάθος
111	Σωστό
112	Λάθος
113	Σωστό
114	Λάθος
115	Λάθος
116	Λάθος
117	Λάθος
118	Λάθος
119	Σωστό
120	Λάθος
121	Λάθος
122	Λάθος
123	Σωστό
124	Σωστό
125	Σωστό
126	Σωστό
127	Λάθος
128	Λάθος

129	Σωστό
130	Λάθος
131	Λάθος
132	Λάθος
133	Σωστό
134	Λάθος
ΚΑΤΑΛΟΓΟΣ ΑΠΑΝΤΗΣΕΩΝ ΣΤΙΣ ΕΡΩΤΗΣΕΙΣ ΑΝΤΙΣΤΟΙΧΙΣΗΣ ΓΙΑ ΤΗΝ ΑΠΟΤΙΜΗΣΗ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ	
A/A Ερώτησης	Σωστή απάντηση
135	1-δ, 2-γ, 3-α, 4-β
136	1-γ, 2-α, 3-β, 4-δ
137	1-α, 2-γ, 3-δ, 4-β
138	1-γ, 2-α, 3-β
139	1-β, 2-α, 3-δ, 4-γ
140	1-γ, 2-δ, 3-α, 4-β
141	1-α, 2-β, 3-γ
142	1-β, 2-α, 3-δ, 4-γ
143	1-β, 2-α, 3-γ, 4-δ
144	1-α, 2-β, 3-γ
145	1-β, 2-γ, 3-δ, 4-α
146	1-δ, 2-γ, 3-β, 4-α
147	1-δ, 2-α, 3-β, 4-γ
148	1-β, 2-γ, 3-α
149	1-α, 2-β, 3-γ
150	1-α, 2-γ, 3-β

5. ΑΠΑΝΤΗΣΕΙΣ ΠΡΑΚΤΙΚΗΣ ΚΑΤΕΥΘΥΝΣΗΣ

ΚΑΤΑΛΟΓΟΣ ΑΠΑΝΤΗΣΕΩΝ ΣΤΙΣ ΕΡΩΤΗΣΕΙΣ ΠΟΛΛΑΠΛΗΣ ΕΠΙΛΟΓΗΣ ΓΙΑ ΤΗΝ ΑΠΟΤΙΜΗΣΗ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ	
A/A Ερώτησης	Σωστή απάντηση
1	γ
2	γ
3	γ
4	δ
5	γ
6	α

7	γ
8	β
9	γ
10	γ
11	α
12	β
13	δ
14	α
15	β
16	δ
17	β
18	β
19	α
20	β
21	γ
22	γ
23	β
24	γ
25	δ
26	γ
27	γ
28	γ
29	γ
30	β

ΚΑΤΑΛΟΓΟΣ ΑΠΑΝΤΗΣΕΩΝ ΣΤΙΣ ΕΡΩΤΗΣΕΙΣ ΣΩΣΤΟΥ - ΛΑΘΟΥΣ ΓΙΑ ΤΗΝ ΑΠΟΤΙΜΗΣΗ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ

A/A Ερώτησης	Σωστή απάντηση
31	Σωστό
32	Σωστό
33	Λάθος
34	Λάθος
35	Λάθος
36	Λάθος
37	Λάθος
38	Λάθος
39	Σωστό
40	Λάθος
41	Σωστό

ΚΑΤΑΛΟΓΟΣ ΑΠΑΝΤΗΣΕΩΝ ΣΤΙΣ ΕΡΩΤΗΣΕΙΣ ΑΝΤΙΣΤΟΙΧΙΣΗΣ ΓΙΑ ΤΗΝ ΑΠΟΤΙΜΗΣΗ ΓΝΩΣΕΩΝ ΚΑΙ ΔΕΞΙΟΤΗΤΩΝ	
A/A Ερώτησης	Σωστή απάντηση
42	1-γ, 2-α, 3-β
43	1-β, 2-α, 3-δ, 4-γ
44	1-α, 2-β, 3-δ, 4-γ
45	1-β, 2-α, 3-δ, 4-γ
46	1-δ, 2-β, 3-α, 4-γ
47	1-α-δ, 2-β-γ
48	1-α, 2-β, 3-γ
49	1-α, 2-β, 3-γ
50	1-α, 2-β, 3-γ, 4-δ