ΕΡΩΤΗΣΗ #01

Για τις ακόλουθες περιπτώσεις επιλέξτε τη σωστή/ές εκφράσεις σχετικά με το κατά πόσον η καθεμιά ενέργεια είναι σύμφωνη ή όχι με καθεμιά από τις τρεις βασικές απαιτήσεις ασφάλειας (εμπιστευτικότητα - Ε, ακεραιότητα - Α, διαθεσιμότητα - Δ), ενώ αιτιολογείτε στη κόλλα την /τις επιλογή/ές σας με βάση τους σχετικούς ορισμούς των Ε, Α και Δ:

i. Μπορεί ένας ιστότοπος να αρνείται τη χρήση των υπηρεσιών του από εξουσιοδοτημένους χρήστες όταν οι συνθήκες το απαιτούν.
ii. Μπορεί ένας χρήστης να τροποποιήσει ένα αρχείο χωρίς να διαθέτει τις απαραίτητες εξουσιοδοτήσεις για κάθε είδους πρόσβαση σε αυτό.
iii. Μπορεί ένας χρήστης Α να διαβάσει τις φωτογραφίες που έχει αναρτήσει ένας άλλος χρήστης Β στη σελίδα κοινωνικής δικτύωσής του για ιδιωτική χρήση.
iv. Μπορεί ένας χρήστης να ζητήσει ενημέρωση από το λειτουργικό σύστημα για τις δυνατότητες άλλων χρηστών να συλλέξουν και να επεξεργαστούν τα δεδομένα που έχει αποθηκεύσει σε αρχεία που του ανήκουν.

α) Δεν είναι σύμφωνες οι i και iv με τις Δ και Α, αντίστοιχα.
β) Δεν είναι σύμφωνες οι iv και iii με τις Α και Ε, αντίστοιχα.
γ) Δεν είναι σύμφωνες οι ii και iv με τις Ε και Α, αντίστοιχα.
δ) Δεν είναι σύμφωνες οι i και iii με τις Δ και Α, αντίστοιχα.
ε) Δεν είναι σύμφωνες οι i και ii με τις Δ και Α, αντίστοιχα.
στ) Δεν είναι σύμφωνες οι iv και iii με τις ΑΔ και Ε, αντίστοιχα.
ζ) Δεν είναι σύμφωνες οι ii και iii με τις Α και Ε, αντίστοιχα.

ΕΡΩΤΗΣΗ #02

Στο εξωτερικό δίκτυο της εταιρείας ACME λειτουργεί το Web server (WS) και ένα Management Workstation (MW), ενώ στο εσωτερικό δίκτυο, μεταξύ άλλων, λειτουργεί το Database Server (DS), στου οποίου τα περιεχόμενα παρέχεται ελεγχόμενη πρόσβαση σε εξωτερικούς χρήστες μέσω του WS, καθώς και απομακρυσμένη πρόσβαση στο διαχειριστή του DS μέσω του MW. Έχετε εντοπίσει στον MW την (υποθετική) ευπάθεια CVE-2024-12 με τιμή CVSS 6,0 που επιτρέπει πρόσβαση με δικαιώματα διαχειριστή και στον WS την (υποθετική) ευπάθεια CVE-2024-23 με τιμή CVSS 5,0 που επιτρέπει την απομακρυσμένη σύνδεση (reverse shell) από χρήστες εκτός δικτύου της ACME. Ακόμη, εκτιμάτε ότι ως πιθανά σενάρια επίθεσης για μη-εξουσιοδοτημένη πρόσβαση στο DS είναι τα εξής:

i. αξιοποίηση της ευπάθειας CVE-2024-12, αφού προηγουμένως γίνει στο MW εγκατάσταση κακόβουλου λογισμικού (drive-by download) μετά από απρόσεκτο χειρισμό μηνύματος email από εξουσιοδοτημένο χρήστη, με αποτέλεσμα την πιθανή απόκτηση πρόσβασης στο DS εφόσον ο διαχειριστής προλάβει να αντιληφθεί την παρείσφρηση όπως έχει συμβεί σε δυο (2) παρόμοιες περιπτώσεις τα τελευταία δέκα (10) χρόνια. Παρόμοια περιστατικά λανθασμένων χειρισμών (ευτυχώς χωρίς επιπτώσεις) έχουν παρατηρηθεί αρκετές φορές τους τελευταίους μήνες, οπότε εκτιμάτε ότι είναι πιθανή η επανάληψή τους στο ένα δέκατο του πλήθους των περιπτώσεων λήψης κακόβουλων μηνυμάτων.
ii. αξιοποίηση της ευπάθειας CVE-2024-23, με αποτέλεσμα τη δυνατότητα απόκτησης πρόσβασης στο DS, αφού πρώτα δοκιμαστούν κατάλληλα σύνολα εντολών (script) με πιθανότητα επιτυχίας 20%.

Αφού σχεδιάσετε στην κόλλα το γράφο επιθέσεων και υπολογίσετε τις σχετικές ενδιάμεσες και τελικές πιθανότητες, να επιλέξτε τη σωστή/ές εκφράσεις για τα αποτελέσματα του υπολογισμού της πιθανότητας να αποκτήσει ένας επιτιθέμενος πρόσβαση στο DS για κάθε ένα σενάριο (p_i και p_{ii}, αντίστοιχα), υποθέτοντας ότι η πιθανότητα αξιοποίησης μιας επίθεσης είναι το ένα δέκατο του αντίστοιχου CVSS.

α) $p_i = 0,2$ και $p_{ii} = 0,5$
β) $p_i = 0,2$ και $p_{ii} = 0,1$
γ) $p_i = 0,5$ και $p_{ii} = 0,6$
δ) $p_i = 0,012$ και $p_{ii} = 0,6$
ε) $p_i = 0,012$ και $p_{ii} = 0,1$
στ) $p_i = 0,5$ και $p_{ii} = 0,5$
ζ) άλλα αποτελέσματα

ΕΡΩΤΗΣΗ #03

Σε συνέχεια της προηγούμενης ερώτησης (#02), να υπολογίσετε στην κόλλα και να επιλέξτε τη σωστή έκφραση για τον υπολογισμό της συνολικής πιθανότητας Σp να αποκτήσει ένας επιτιθέμενος πρόσβαση στο DS.

α) $\Sigma p = 0,6048$
β) $\Sigma p = 0,1108$
γ) $\Sigma p = 0,6$
δ) $\Sigma p = 0,8$
ε) $\Sigma p = 0,75$
στ) $\Sigma p = 0,28$
ζ) άλλο αποτέλεσμα

ΕΡΩΤΗΣΗ #04

Ποιος είναι ο σκοπός ενός συστήματος διαχείρισης ταυτότητας και πρόσβασης (identity and access management);

α) Να καταργήσει τη χρήση συνθηματικών κατά την αυθεντικοποίηση.
β) Να παρέχει τα στοιχεία των ταυτοτήτων σε μία ή περισσότερες εφαρμογές.
γ) Να εφαρμόζει πολιτικές ασφάλειας σε μία ή περισσότερες εφαρμογές.
δ) Να παρέχει τα στοιχεία των ταυτοτήτων και να εφαρμόζει πολιτικές ασφάλειας σε μία ή περισσότερες εφαρμογές.

ΕΡΩΤΗΣΗ #05

Επιλέξτε τη σωστή συνέχεια της φράσης, με κατάλληλη αιτιολόγηση στην κόλλα: Με την εντολή GRANT

```
CFO TO PROF WITH GRANT OPTION,
```

α) δεν αλλάζει κάτι για το PROF γιατί υπάρχει λάθος στην εντολή
β) το PROF μπορεί να εκχωρήσει το CFO
γ) το PROF μπορεί να εκχωρήσει προνόμια στο CFO
δ) το PROF μπορεί να διαγράψει το CFO

ΕΡΩΤΗΣΗ #06

Η Alice και ο Bob εργάζονται στην ίδια επενδυτική εταιρεία. Η Alice έχει διαβάσει τα ευαίσθητα (unsanitized) δεδομένα της σοκολατοποιΐας ΙΟΝ και της μεταφορικής ΑΤΛΑΣ. Ο Bob έχει διαβάσει τα ευαίσθητα (unsanitized) δεδομένα της σοκολατοποιΐας ΠΑΥΛΙΔΗΣ. Σύμφωνα με το μοντέλο ασφάλειας Chinese Wall, ποια(ες) από τις ακόλουθες ενέργειες είναι επιτρεπτή(ές); Να αναφέρετε στην κόλλα το λόγο της κάθε επιλογής σας.

α) Η Alice μπορεί να γράψει στα unsanitized δεδομένα της μεταφορικής ΑΣΤΡΑΠΗ
β) Η Alice μπορεί να διαβάσει τα unsanitized δεδομένα της σοκολατοποιΐας NESTLE
γ) Η Alice μπορεί να διαβάσει τα sanitized δεδομένα της σοκολατοποιΐας ΠΑΥΛΙΔΗΣ
δ) Ο Bob μπορεί να διαβάσει τα unsanitized δεδομένα της μεταφορικής ΑΤΛΑΣ
ε) Ο Bob μπορεί να διαβάσει τα sanitized δεδομένα της μεταφορικής ΑΤΛΑΣ

ΕΡΩΤΗΣΗ #07

Ο χρήστης Γ έχει διαβάθμιση Διαβαθμισμένο και εργάζεται στο έργο Μετρό Αθήνας. Ο χρήστης Δ έχει διαβάθμιση Διαβαθμισμένο και εργάζεται στο έργο Μετρό Θεσσαλονίκης. Ο χρήστης Β έχει διαβάθμιση Απόρρητο και εργάζεται στο έργο Μετρό Μακεδονίας. Ο χρήστης Α έχει διαβάθμιση Άκρως Απόρρητο και εργάζεται στο έργο Μετρό Ελλάδας. Οι γεωγραφικοί προσδιορισμοί στους τίτλους των έργων συνεπάγονται ενδεχόμενες συμπεριλήψεις κατηγοριών (π.χ. το έργο Μετρό Θεσσαλονίκης συμπεριλαμβάνεται σε αυτό του Μετρό Μακεδονίας και αυτό στο έργο του Μετρό Ελλάδας). Ο χρήστης Α δημιουργεί το αρχείο f1, ο χρήστης Β δημιουργεί το αρχείο f2 και ο χρήστης Γ δημιουργεί το αρχείο f3. Ποια(ες) από τις ακόλουθες ενέργειες είναι επιτρεπτή(ές) ή όχι, σύμφωνα με το μοντέλο Bell-LaPadula; Να αναφέρετε στην κόλλα το λόγο της κάθε επιλογής σας.

α) Ο χρήστης Γ γράφει στο αρχείο f2.
β) Ο χρήστης Α διαβάζει τα f2 και f3 και γράφει στο f1.
γ) Ο χρήστης Β διαβάζει το f3.
δ) Ο χρήστης Δ διαβάζει το f3.
ε) Ο χρήστης Β δημιουργεί νέο αρχείο f4 ως Άκρως Απόρρητο.

ΕΡΩΤΗΣΗ #08

Ο οργανισμός ACME έχει κάνει τις ακόλουθες εκτιμήσεις για τις ακόλουθες απειλές κατά αγαθών του πληροφοριακού του συστήματος, την αξία του απειλούμενου αγαθού (ΑΑΑ), τον συντελεστή επίπτωσης (ΣΕΠ), καθώς και τη συχνότητα εμφάνισης της κάθε απειλής (ΣΕΑ):

	Απειλή	ΑΑΑ	ΣΕΠ	ΣΕΑ
i.	Επίθεση τύπου ransomware	75000 €	0,3	Μία φορά κάθε 4 μήνες
ii.	Διαγραφή αρχείων από λάθος	10000 €	0,1	Μία φορά ανά τρίμηνο
iii.	Driven-by download	3000 €	0,6	Δύο φορές κάθε 3 χρόνια
iv.	Κλοπή εξοπλισμού	500 €	1	2 φορές το μήνα

Επιλέξτε το συνδυασμό με τις σωστές τιμές ALE (Annualized Loss Expectancy):

α) i. 3000, ii. 100000, iii. 2700, iv. 12000
β) i. 12000, ii. 50000, iii. 5400, iv. 3000
γ) i. 75000, ii. 4000, iii. 2700, iv. 12000
δ) i. 12000, ii. 75000, iii. 5400, iv. 3000
ε) i. 75000, ii. 3000, iii. 2700, iv. 12000
στ) i. 150000, ii. 6000, iii. 5400, iv. 3000
ζ) i. 12000, ii. 100000, iii. 2700, iv. 6000

ΕΡΩΤΗΣΗ #09

Αν για τον (υπο)κατάλογο exams θέλετε να διαθέτει προνόμιο εκτέλεσης τουλάχιστον η ομάδα, κατάλληλη/ες εντολή/ές (πριν ή μετά τη δημιουργία του) είναι (παραθέστε όλους τους σχετικούς υπολογισμούς στην κόλλα):

α) umask 666
β) umask 613
γ) umask 400
δ) umask 531
ε) chmod a+x exams
στ) chmod g+x exams
ζ) chmod o-x exams

ΕΡΩΤΗΣΗ #10

Επιλέξτε τη σωστή συνέχεια της φράσης, με κατάλληλη αιτιολόγηση στην κόλλα: Με την εντολή **REVOKE CFO FROM PROF**,

α) ανακαλούνται όλα τα προνόμια μόνο του CTO
β) ανακαλούνται όλα τα προνόμια του CTO και των junior ρόλων που δεν έχουν εκχωρηθεί ρητά στο PROF
γ) ανακαλούνται όλα τα προνόμια του CTO και των junior ρόλων που έχουν εκχωρηθεί ρητά στο PROF
δ) δεν ανακαλούνται τα προνόμια αν ο CTO προστατεύεται από συνθηματικό

- Καλή Επιτυχία -