ΘΕΜΑΤΑ ΕΞΕΤΑΣΕΩΝ ΙΟΥΝΙΟΥ 2024
ΤΜΗΜΑ: ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΜΑΘΗΜΑ: ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ

A

**ΕΠΩΝΥΜΟ:** _____ **ΟΝΟΜΑ:** _____

**Ιδρυματική διεύθυνση email:** _____

**ΟΔΗΓΙΕΣ:** Για να απαντήσετε τις ερωτήσεις που ακολουθούν:
1) Συμπληρώνετε κατάλληλα το Απαντητικό Δελτίο, στο τέλος (υπάρχουν σχετικές οδηγίες και εκεί).
2) Αποτυπώνετε αναλυτικά στην κόλλα το σχετικό υπολογισμό ή αιτιολόγηση ανά ερώτηση (φροντίζετε ώστε να είναι ευκρινής η διευκρινιστική αναγραφή, π.χ. ΕΡΩΤΗΣΗ #05).

**ΕΡΩΤΗΣΗ #01**
Με την εντολή GRANT STD TO CFO WITH ADMIN OPTION
α) Δεν αλλάζει κάτι για το CFO γιατί υπάρχει λάθος στην εντολή;
β) Το CFO μπορεί να εκχωρήσει το STD;
γ) Το CFO μπορεί να εκχωρήσει προνόμια στο STD;
δ) Το CFO μπορεί να διαγράψει το STD
ε) Άλλο

**ΕΡΩΤΗΣΗ #02**
Με την εντολή REVOKE STD FROM CFO
α) Ανακαλούνται από CFO όλα τα προνόμια μόνο του STD;
β) Ανακαλούνται από CFO όλα τα προνόμια του STD και των junior ρόλων που έχουν εκχωρηθεί ρητά στο CFO;
γ) Ανακαλούνται από CFO όλα τα προνόμια του STD και των junior ρόλων που έχουν εκχωρηθεί στο STD;
δ) Δεν ανακαλούνται τα προνόμια αν το STD προστατεύεται από συνθηματικό;
ε) Άλλο

**ΕΡΩΤΗΣΗ #03**
Επιλέξτε την/τις σωστή/ές χρησιμότητα/ες της σύνοψης (hash) ενός δίσκου ή επιμέρους αρχείων του:

α) Απόδειξη ότι δεν παραχαράχθηκε το περιεχόμενο του δίσκου πριν και μετά την εξέτασή του.
β) Προστασία με χρήση κρυπτογραφίας.
γ) Εντοπισμός ύποπτων ή αναζητούμενων αρχείων.
δ) Ψευδονυμοποίηση του περιεχομένου τους.
ε) Μείωση του μεγέθους του αντιγράφου του δίσκου.

**ΕΡΩΤΗΣΗ #04**

Το πεδίο ορισμού ασφάλειας (security domain) ενός (απλού, όχι του διαχειριστή) χρήστη κατά τη διάρκεια μιας συνόδου (session) συμπεριλαμβάνει:

α) τα προνόμια αντικειμένων σε όλα τα αντικείμενα του σχήματός του;
β) τα προνόμια συστήματος σε όλα τα αντικείμενα του σχήματός του;
γ) τα προνόμια συστήματος που του έχουν παραχωρηθεί;
δ) τα προνόμια αντικειμένων για αντικείμενα άλλων σχημάτων που του έχουν παραχωρηθεί με WITH ADMIN;
ε) τα προνόμια από τους ρόλους που του έχουν παραχωρηθεί, αμέσως μετά την εκτέλεση της σχετικής εντολής GRANT από τον grantor;
στ) τα προνόμια που έχουν παραχωρηθεί στην ομάδα χρηστών PUBLIC;

**ΕΡΩΤΗΣΗ #05**

Για τις απειλές κατά ορισμένων αγαθών του πληροφοριακού σας συστήματος
συνέχεια, ο οργανισμός σας έχει κάνει τις ακόλουθες εκτιμήσεις αναφορικά με τη συχνότητα τους και τη
οικονομική ζημία που επιφέρουν:

| Απειλή | Αναμενόμενη οικονομική ζημιά σε περίπτωση εκδήλωσης απειλής | Συχνότητα εμφάνισης απειλής |
|---|---|---|
| i. Κλοπή εξοπλισμού | 500 € | 2 φορές το μήνα |
| ii. Επίθεση τύπου sql injection στη βάση δεδομένων | 25000 € | Μία φορά κάθε 4 μήνες |
| iii. Πειρατεία λογισμικού | 1800 € | Δύο φορές κάθε 3 χρόνια |
| iv. Διαγραφή αρχείων από ανθρώπινο λάθος | 1000 € | Μία φορά ανά τρίμηνο |

ΣΕΠ
1
1
1
1

Επιλέξτε το συνδυασμό με τις σωστές τιμές ALE:

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

**ΕΡΩΤΗΣΗ #06**

Με ποια εντολή θα μπορούσατε να διαμορφώσετε τα κατάλληλα προνόμια σε έναν κατάλογο στον οποίο θα μπορούν να τοποθετούν οι χρήστες τα αρχεία τους, χωρίς όμως να μπορούν να διαβάσουν ο ένας τα αρχεία του άλλου;

α) chmod 222 alldir
β) chmod 333 alldir
γ) chmod 444 alldir
δ) chmod 555 alldir
ε) Άλλη εντολή.

**ΕΡΩΤΗΣΗ #07**

Επιλέξτε τη/τις σωστή/ές προτάσεις, θεωρώντας ότι έχουν εκτελεστεί οι ακόλουθες εντολές SQL από το διαχειριστή DBA και τον απλό χρήστη TELLER1:

```
DBA> CREATE ROLE LOANS;

DBA> GRANT CREATE VIEW TO LOANS;

DBA> GRANT LOANS TO TELLER2;

TELLER1> GRANT SELECT ON INCOM TO LOANS;

TELLER1> GRANT SELECT ON OUTCOM TO TELLER2;
```

α) ο χρήστης TELLER2 μπορεί να εκτελέσει εντολές SELECT στο INCOM
β) ο χρήστης TELLER2 δεν μπορεί να εκτελέσει εντολές SELECT στο OUTCOM
γ) ο χρήστης TELLER2 διαθέτει το προνόμιο CREATE VIEW
δ) ο χρήστης TELLER2 δεν μπορεί να δημιουργήσει μια άποψη που αναφέρεται στο INCOM
ε) ο χρήστης TELLER2 μπορεί να δημιουργήσει μια άποψη που αναφέρεται στο INCOM
στ) ο χρήστης TELLER2 δεν μπορεί να δημιουργήσει μια άποψη που αναφέρεται στο OUTCOM
ζ) ο χρήστης TELLER2 μπορεί να δημιουργήσει μια άποψη που αναφέρεται στο OUTCOM

**ΕΡΩΤΗΣΗ #08**

Ποιο είναι το νόημα του προνομίου εκτέλεσης σε έναν κατάλογο στο ΛΣ Linux;

α) Είναι δυνατή η εκτέλεση των αρχείων που περιέχει.
β) Είναι δυνατή η ανάγνωση των περιεχομένων του.
γ) Είναι δυνατή η μετάβαση στον κατάλογο αυτό.
δ) Είναι δυνατή η μετατροπή των αρχείων που περιέχει.
ε) Κανένα. Πρέπει οπωσδήποτε να συνοδεύεται από ένα ακόμη προνόμιο.

**ΕΡΩΤΗΣΗ #09**

Αν θέλετε σε ένα νέο αρχείο να διαθέτει προνόμιο εκτέλεσης η ομάδα, τότε πρέπει να δώσετε (επιλέξτε μια ή περισσότερες εντολές):

α) chmod +x μετά τη δημιουργία του αρχείου
β) umask 022 πριν τη δημιουργία του αρχείου
γ) umask 711 πριν τη δημιουργία του αρχείου
δ) umask 666 πριν τη δημιουργία του αρχείου
ε) umask 070 πριν τη δημιουργία του αρχείου
στ) Άλλη εντολή.

**ΕΡΩΤΗΣΗ #10**

Για τις ακόλουθες ενέργειες 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):

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

**ΕΡΩΤΗΣΗ #11**

Το εταιρικό δίκτυο της ACME περιλαμβάνει δυο υποδίκτυα: το εξωτερικό και το εσωτερικό. Στο εξωτερικό υπάρχει ένας εξυπηρετητής διαδικτύου (ΕΔ) και ένας υπολογιστής διαχείρισης (ΥΔ). Στο εσωτερικό βρίσκεται ένας εξυπηρετητής βάσης δεδομένων (ΕΒ), στου οποίου τα περιεχόμενα παρέχεται ελεγχόμενη πρόσβαση σε εξωτερικούς χρήστες μέσω του ΕΔ, καθώς και πρόσβαση στο διαχειριστή της βάσης δεδομένων μέσω του ΥΔ. Στον ΥΔ υπάρχει η (υποθετική) ευπάθεια CVE-2024-a με τιμή CVSS 8,3 που επιτρέπει πλήρη πρόσβαση (privilege escalation) και στον ΕΔ υπάρχει η (υποθετική) ευπάθεια CVE-2024-b με τιμή CVSS 7,1 που επιτρέπει απομακρυσμένη εκτέλεση εντολών (remote command execution). Έχετε διαπιστώσει ως πιθανά σενάρια επίθεσης για μη-εξουσιοδοτημένη πρόσβαση στο ΕΒ τα εξής:

i. αξιοποίηση της ευπάθειας CVE-2024-a, αφού προηγουμένως γίνει στο ΥΔ εγκατάσταση κακόβουλου λογισμικού με λανθασμένο χειρισμό μηνύματος email από εξουσιοδοτημένο χρήστη, με αποτέλεσμα τη βέβαιη απόκτηση πρόσβασης στο ΕΒ. 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-b, με αποτέλεσμα τη δυνατότητα απόκτησης πρόσβασης στο ΕΒ εφόσον δοκιμαστούν κατάλληλες εντολές με πιθανότητα επιτυχίας 40%.

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 των πιθανοτήτων να αποκτήσει ένας επιτιθέμενος πρόσβαση στο ΕΒ για κάθε ένα σενάριο ($p_i$ και $p_{ii}$, αντίστοιχα), υποθέτοντας ότι η πιθανότητα αξιοποίησης μιας ευπάθειας είναι το ένα δέκατο του αντίστοιχου CVSS.

α) $p_i = 0{,}830$ και $p_{ii} = 0{,}284$
β) $p_i = 0{,}083$ και $p_{ii} = 0{,}284$
γ) $p_i = 0{,}284$ και $p_{ii} = 0{,}830$
δ) $p_i = 1$ και $p_{ii} = 0{,}284$
ε) $p_i = 0{,}83$ και $p_{ii} = 0{,}71$
στ) $p_i = 0{,}1$ και $p_{ii} = 0{,}4$
ζ) Άλλο

**ΕΡΩΤΗΣΗ #12**

Σε συνέχεια της προηγούμενης ερώτησης (11), επιλέξτε τη σωστή/ές εκφράσεις για τα αποτελέσματα του υπολογισμού της συνολικής πιθανότητας Σp (είτε με το ένα είτε με το άλλο σενάριο).

α) $\Sigma p = 0{,}0235$
β) $\Sigma p = 0{,}0400$
γ) $\Sigma p = 0{,}8783$
δ) $\Sigma p = 0{,}2358$
ε) $\Sigma p = 0{,}3434$
στ) $\Sigma p = 0{,}9507$
ζ) Άλλο

**- Καλή Επιτυχία -**