ΘΕΜΑΤΑ ΕΞΕΤΑΣΕΩΝ ΙΟΥΝΙΟΥ 2022
ΤΜΗΜΑ: ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΜΑΘΗΜΑ: ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ

A

ΕΡΩΤΗΣΗ #01

Με την εντολή GRANT CTO TO STUDENT WITH ADMIN OPTION

1) Δεν αλλάζει κάτι για το STUDENT γιατί υπάρχει λάθος στην εντολή;
2) Το STUDENT μπορεί να εκχωρήσει το CTO;
3) Το STUDENT μπορεί να εκχωρήσει προνόμια στο CTO;
4) Το STUDENT μπορεί να διαγράψει το CTO

ΕΡΩΤΗΣΗ #02

Με την εντολή REVOKE CTO FROM STUDENT

1) Ανακαλούνται όλα τα προνόμια μόνο του CTO;
2) Ανακαλούνται όλα τα προνόμια του CTO και των junior ρόλων που έχουν εκχωρηθεί ρητά στο STUDENT;
3) Ανακαλούνται όλα τα προνόμια του CTO και των junior ρόλων που δεν έχουν εκχωρηθεί ρητά στο STUDENT;
4) Δεν ανακαλούνται τα προνόμια αν ο CTO προστατεύεται από συνθηματικό.

ΕΡΩΤΗΣΗ #03

Επιλέξτε τους σωστούς συνδυασμούς για τα χαρακτηριστικά

- ΠΩ: Πολυπλοκότητα Χώρου
- ΠΡ: Πολυπλοκότητα Χρόνου
- ΤΑ: Τελικό Αποτέλεσμα

των επιθέσεων ανάκτησης συνθηματικού εξαντλητικής αναζήτησης (brute force) και λεξικού (dictionary):

1) Brute force: ΠΩ=Υψηλό, ΠΡ=Υψηλό, ΤΑ= Αβέβαιο;
2) Dictionary: ΠΩ=Υψηλό, ΠΡ= Χαμηλό, ΤΑ= Σίγουρο;
3) Dictionary: ΠΩ=Υψηλό, ΠΡ=Υψηλό, ΤΑ= Αβέβαιο;
4) Dictionary: ΠΩ=Υψηλό, ΠΡ= Χαμηλό, ΤΑ= Αβέβαιο;
5) Dictionary: ΠΩ= Χαμηλό, ΠΡ=Υψηλό, ΤΑ= Σίγουρο;
6) Brute force: ΠΩ=Χαμηλό, ΠΡ=Υψηλό, ΤΑ= Αβέβαιο;
7) Brute force: ΠΩ=Χαμηλό, ΠΡ=Υψηλό, ΤΑ= Σίγουρο;
8) Brute force: ΠΩ= Χαμηλό, ΠΡ=Υψηλό, ΤΑ= Αβέβαιο

ΕΡΩΤΗΣΗ #04

Επιλέξτε τα σωστά αποτελέσματα (σε συμβολική μορφή) της εκτέλεσης της εντολής `umask 012` για τα προνόμια νέων αρχείων και νέων καταλόγων (κάνετε 2 επιλογές):

1) rw-rw-r-x
2) rw-r--r--
3) rwxrw-r-x
4) rw-r--rw-
5) rwxrwxr-x
6) rw-rw-r--
7) rw-rwxr-x
8) rw-rw-rw-

ΕΡΩΤΗΣΗ #05

Το πεδίο ορισμού ασφάλειας (security domain) ενός (απλού, όχι του διαχειριστή) χρήστη συμπεριλαμβάνει:

1) τα προνόμια αντικειμένων σε όλα τα αντικείμενα του σχήματός του.
2) τα προνόμια συστήματος σε όλα τα αντικείμενα του σχήματός του.
3) τα προνόμια συστήματος που έχουν παραχωρηθεί στον χρήστη.
4) τα προνόμια αντικειμένων για αντικείμενα άλλων σχημάτων που έχουν παραχωρηθεί στον χρήστη.
5) τα προνόμια των ρόλων που έχουν παραχωρηθεί στον χρήστη και είναι ενεργοποιημένοι.
6) τα προνόμια και τους ρόλους που έχουν παραχωρηθεί στην ομάδα χρηστών PUBLIC.

ΕΡΩΤΗΣΗ #06

Ένας υπολογιστής χωρίς προστασία antimalware που είναι συνδεμένος στο διαδίκτυο έχει μολυνθεί τουλάχιστον 3 φορές στα 5 χρόνια. Ο συντελεστής επίπτωσης στην αξία των δεδομένων στον υπολογιστή, η οποία ανέρχεται σε 1000 ευρώ, λόγω της πραγματοποίησης μιας απειλής malware είναι 80%. Αν το ετήσιο κόστος χρήσης ενός λογισμικού προστασίας antimalware είναι €500, η απόφαση διαχείρισης της επικινδυνότητας που προκύπτει με βάση τον υπολογισμό του ALE (Annualized Loss Expectancy) είναι:

1) Αρνητικό για αγορά του λογισμικού προστασίας γιατί προκύπτει ALE < 500;
2) Ουδέτερο ως προς την αγορά του λογισμικού προστασίας γιατί προκύπτει ALE = 500;
3) Θετικό για αγορά του λογισμικού προστασίας γιατί προκύπτει ALE > 500;
4) Η απόφαση δεν σχετίζεται με τις παραπάνω επιλογές.

ΕΡΩΤΗΣΗ #07

Επιλέξτε τους σωστούς συνδυασμούς για τα χαρακτηριστικά των δομών ελέγχου προσπέλασης Λίστες Ελέγχου Προσπέλασης (ΛΕΠ) και Πίνακες Ελέγχου Προσπέλασης (ΠΕΠ):

1) Εύκολη προσθήκη δικαιωμάτων προσπέλασης για νέο υποκείμενο: ΠΕΠ
2) Εύκολη μεταβολή δικαιωμάτων προσπέλασης για νέο υποκείμενο: ΛΕΠ
3) Εύκολη διαγραφή δικαιωμάτων προσπέλασης ενός υποκειμένου: ΠΕΠ
4) Εύκολη προσθήκη νέου αντικειμένου για πρόσβαση από όλα τα υποκείμενα: ΛΕΠ
5) Δύσκολη διαγραφή δικαιωμάτων προσπέλασης ενός υποκειμένου: ΠΕΠ

ΕΡΩΤΗΣΗ #08

Η σχέση επικράτησης (dominance) στο lattice model ικανοποιεί τις ακόλουθες ιδιότητες:

1) Μεταβατική
2) Προσεταιριστική
3) Αντισυμμετρική
4) Πληρότητα
5) Αντανακλαστική

ΕΡΩΤΗΣΗ #09

Με ποιαν εντολή θα μπορούσατε να «αποκρύψετε» την ύπαρξη ενός καταλόγου μέσα σε έναν άλλο (π.χ. /eagle/r2/dlsdir), επιτρέποντας όμως σε αυτούς που γνωρίζουν την ύπαρξή του να τον χρησιμοποιήσουν

1) chmod a=x /eagle/r2

2) chmod a=r /eagle/r2
3) chmod a=x /eagle/r2/dlsdir
4) chmod a=r /eagle/r2/dlsdir
5) Άλλη εντολή.

ΕΡΩΤΗΣΗ #10

Επιλέξτε τη σωστή/ές εκφράσεις για τα αποτελέσματα των παραχωρήσεων προνομίων και ρόλων στο ΣΔΒΔ Oracle:

1) Η παραχώρηση προνομίου γίνονται εμφανής αμέσως.
2) Οι παραχωρήσεις προνομίου γίνονται εμφανείς μόνον όταν ενεργοποιηθούν οι εκχωρημένοι ρόλοι.
3) Η παραχώρηση ρόλου γίνεται εμφανής όταν ο αποδέκτης ξεκινήσει κατόπιν μια νέα σύνοδο.
4) Η παραχώρηση ενός ρόλου γίνεται εμφανής όταν ο αποδέκτης ενεργοποιήσει τον ρόλο.

ΕΡΩΤΗΣΗ #11

Αν θέλετε σε ένα νέο αρχείο να διαθέτει προνόμιο εκτέλεσης η ομάδα, τότε πρέπει να δώσετε:

1) chmod g+x μετά τη δημιουργία του αρχείου
2) umask 022 πριν τη δημιουργία του αρχείου
3) umask 711 πριν τη δημιουργία του αρχείου
4) umask 666 πριν τη δημιουργία του αρχείου
5) umask 070 πριν τη δημιουργία του αρχείου

ΕΡΩΤΗΣΗ #12

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 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.

1) Δεν είναι σύμφωνες οι i και iv με τις Δ και Α, αντίστοιχα.
2) Δεν είναι σύμφωνες οι i και ii με τις Δ και Α, αντίστοιχα.
3) Δεν είναι σύμφωνες οι ii και iii με τις Α και Ε, αντίστοιχα.
4) Δεν είναι σύμφωνες οι iv και iii με τις Α και Ε, αντίστοιχα.
5) Δεν είναι σύμφωνες οι ii και iv με τις Ε και Α, αντίστοιχα.
6) Δεν είναι σύμφωνες οι i και iii με τις Δ και Α, αντίστοιχα.
7) Δεν είναι σύμφωνες οι iv και iii με τις ΑΔ και Ε, αντίστοιχα.

ΕΡΩΤΗΣΗ #13

Χρειάζεται να υλοποιήσετε μια πολιτική που θα αποτρέπει την εύρεση των κωδικών με την μέθοδο brute force (εξαντλητική αναζήτηση). Ποιά/ές από τις εξής πολιτικές θα ακολουθούσατε, γνωρίζοντας ότι οι χρήστες εφαρμόζουν πιστά τις οδηγίες σας για ορθή χρήση των συστημάτων;

1) Μέγιστη διάρκεια συνθηματικού τριάντα (30) μέρες
2) Επιβολή ιστορικού συνθηματικού οκτώ (8) θέσεων
3) Ελάχιστη διάρκεια συνθηματικού πέντε (5) μέρες
4) Μέγιστο μήκος συνθηματικού δεκαέξι (16) χαρακτήρες
5) Ελάχιστο μήκος συνθηματικού δέκα (10) χαρακτήρες
6) Αν ο λογαριασμός χρήστη κλειδώσει, τότε αυτό διαρκεί πέντε (5) λεπτά
7) Ο λογαριασμός χρήστη κλειδώνει μετά από τέσσερις (4) αποτυχημένες προσπάθειες
8) Τα συνθηματικά πρέπει να τηρούν τις προϋποθέσεις πολυπλοκότητας (υποχρεωτική χρήση γραμμάτων μικρών και κεφαλαίων, ψηφίων και σημείων στίξης)

ΕΡΩΤΗΣΗ #14

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-2023-a με τιμή CVSS 8,3 που επιτρέπει πλήρη πρόσβαση (privilege escalation) και στον ΕΔ υπάρχει η (υποθετική) ευπάθεια CVE-2023-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-2023-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-2023-b, με αποτέλεσμα τη δυνατότητα απόκτησης πρόσβασης στο ΕΒ εφόσον δοκιμαστούν κατάλληλες εντολές με πιθανότητα επιτυχίας 40%.

Επιλέξτε τη σωστή/ές εκφράσεις για τα αποτελέσματα του υπολογισμού των πιθανότητας 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.

1) $p_i = 0,830$ και $p_{ii} = 0,284$
2) $p_i = 0,083$ και $p_{ii} = 0,284$
3) $p_i = 0,284$ και $p_{ii} = 0,830$
4) $p_i = 1$ και $p_{ii} = 0,284$
5) $p_i = 0,83$ και $p_{ii} = 0,71$
6) $p_i = 0,1$ και $p_{ii} = 0,4$

ΕΡΩΤΗΣΗ #15

Σε συνέχεια της προηγούμενης ερώτησης (14), επιλέξτε τη σωστή/ές εκφράσεις για τα αποτελέσματα του υπολογισμού της συνολικής πιθανότητας Σp (είτε με το ένα είτε με το άλλο σενάριο).

1) $\Sigma p = 0,0235$
2) $\Sigma p = 0,0400$
3) $\Sigma p = 0,8783$
4) $\Sigma p = 0,2358$
5) $\Sigma p = 0,3434$
6) $\Sigma p = 0,9507$

- Καλή Επιτυχία -