ΛΣ Θέμα 2 Κεφ.5

21411.3 Αντιστοιχίστε τα σενάρια της πρώτης στήλης του ακόλουθου πίνακα με τις κατηγορίες χάκερ που αναγράφονται στην δεύτερη στήλη.

Α1. Ανακάλυψη κενού ασφαλείας σε Λειτουργικό Σύστημα και ενημέρωση της ομάδας ανάπτυξης για τη διόρθωσή του.	Β1. Black hats
Α2. Επίθεση κοινωνικής μηχανικής για την απόκτηση κωδικών πρόσβασης σε τραπεζικούς λογαριασμούς και αφαίρεση χρημάτων από αυτούς.	Β2. White hats
Α3. Επίθεση σε ιστότοπο ηλεκτρονικού καταστήματος με σκοπό τη διακοπή της λειτουργίας του και την πρόκληση οικονομικής ζημιάς.	Β3. Grey hats
Α4. Επίθεση σε ιστοσελίδα κυβερνητικού οργανισμού με σκοπό την προβολή σε αυτήν μηνύματος με πολιτικό περιεχόμενο.	
Α5. Επίθεση σε πληροφοριακό σύστημα επιχείρησης με σκοπό την πληροφόρηση των υπευθύνων για την ύπαρξη ευπαθειών.	
Α6. Επίθεση σε υπολογιστικά συστήματα ατόμων που παράγουν και διακινούν κακόβουλο λογισμικό.	

Κ-5.1

18045.1. Οι σύγχρονες στρατηγικές λήψης αντιγράφων ασφαλείας είναι αυτές της λήψης εικόνων των δίσκων (disk image) από ένα υπολογιστικό σύστημα. Αντιστοιχίστε τις στρατηγικές αυτές από την στήλη Α, με τα πλεονεκτήματα που παρέχουν στο σύστημα από την στήλη Β.

Α. Σύγχρονες Στρατηγικές λήψης αντιγράφων ασφαλείας	**Β. Πλεονεκτήματα που παρέχουν**
Α1. Χρήση Εικονικοποιημένων Διακομιστών (Server Virtualization)	Β1. μεγάλος αποθηκευτικός χώρος με χαμηλό κόστος
Α2. Αποθήκευση στο Νέφος (Cloud Storage)	Β2. εύκολη μεταφορά
	Β3. μπορεί να συνεχίσει την λειτουργία του σχεδόν άμεσα, εάν προκύψει hardware πρόβλημα.
	Β4.αυτοματοποιείται η διαδικασία Αντιγράφων Ασφαλείας
	Β5. μειώνει την ανάγκη ύπαρξης διαφορετικών χώρων για την αποθήκευση των Αντιγράφων Ασφαλείας.
	Β6. βοηθά στο να επιτευχθεί γρηγορότερα διαθεσιμότητα του συστήματος
	Β7. μειώνεται η ανάγκη Υλικού (Hardware) και χώρου τοποθέτησής τους

Κ-5.2

18045.2. Έστω πως το Σαββατοκύριακο σε κάποιο υπολογιστικό σύστημα γίνεται το πλήρες αντίγραφο ασφαλείας (full Backup).
Την Δευτέρα τροποποιήθηκε το αρχείο Α , την Τετάρτη το αρχείο Β και το αρχείο Γ, ενώ την Πέμπτη, πάλι το αρχείο Β.
α) Τι θα πάρει το αυξητικό αντίγραφο ασφαλείας (incremental backup) την Τετάρτη (μον 4) και
β) Τι θα πάρει το διαφορικό αντίγραφο ασφαλείας (differential backup) την Πέμπτη (μον 5);

Κ-5.2

18014.2. Στον υπολογιστή του λογιστηρίου μιας εταιρείας είναι αποθηκευμένα τα αρχεία Α, Β, Γ και Δ. Ο παρακάτω πίνακας δείχνει πότε τροποποιούνται τα αρχεία αυτά κατά την διάρκεια 4 εβδομάδων. Τα

αρχεία τροποποιούνται κατά τις εργάσιμες ημέρες ενώ στο τέλος κάθε εβδομάδας, το Σάββατο, δημιουργούνται τα αντίγραφα ασφαλείας.

	1η Εβδομάδα	2η Εβδομάδα	3η Εβδομάδα	4η Εβδομάδα
Α	✓		✓	
Β			✓	
Γ		✓		
Δ				✓

Α) Πότε είναι προτιμότερο ο διαχειριστής του υπολογιστή να πάρει αυξητικό αντίγραφο ασφαλείας (incremental backup) που θα περιέχει τα αρχεία Α και Γ;
Β) Πότε πρέπει να πάρουμε αντίγραφο ασφαλείας που θα περιέχει όλα τα τροποποιημένα αρχεία, και τι είδους αντίγραφο ασφαλείας μπορεί να είναι αυτό;

Κ-5.2

17987.1. Αντιστοιχείστε κατάλληλα τις ΠΕΡΙΠΤΩΣΕΙΣ ΕΛΕΓΧΟΥ ΤΗΣ ΠΡΟΣΒΑΣΗΣ από την στήλη Α με τις ΕΝΕΡΓΕΙΕΣ ΤΩΝ ΧΡΗΣΤΩΝ που αυτές να αφορούν και βρίσκονται στη στήλη Β.

Α. ΠΕΡΙΠΤΩΣΕΙΣ ΕΛΕΓΧΟΥ ΤΗΣ ΠΡΟΣΒΑΣΗΣ	**Β. ΕΝΕΡΓΕΙΕΣ ΤΩΝ ΧΡΗΣΤΩΝ**
Α1. Πρόσβαση σε συστήματα	Β1. Χρησιμοποιούν δικτυακούς εκτυπωτές
Α2. Δικτυακή πρόσβαση	Β2. Έχουν πρόσβαση να διαβάζουν και να τροποποιούν αρχεία
Α3. Πρόσβαση στα δεδομένα	Β3. Χρησιμοποιούν ένα διαμοιραζόμενο σκληρό δίσκο σε ένα δίκτυο
	Β4. Ενημερώνουν μια κοινή για όλους Βάση Δεδομένων
	Β5. Μπορούν να χρησιμοποιούν τα στοιχεία σύνδεσης τους για να συνδεθούν από διαφορετικούς και πολλούς υπολογιστές
	Β6. Έχουν την δυνατότητα να βλέπουν τα μηνύματα άλλων στο δίκτυο

Κ-5.2

17987.2. Σε ένα κατάστημα που εμπορεύεται ηλεκτρονικά είδη υπάρχει ένας υπολογιστής σε κοινόχρηστο χώρο όπου καταχωρούνται οι παραγγελίες των πελατών που το επισκέπτονται.
Ο υπάλληλος που αναλαμβάνει την καταχώριση και την εκτέλεση των παραγγελιών δεν χρησιμοποιεί κωδικούς για την σύνδεσή του στον υπολογιστή αλλά ούτε και στο σχετικό πρόγραμμα, ενώ τον χρόνο που δεν εξυπηρετεί πελάτες παίζει παιχνίδια, στον υπολογιστή αυτόν, που "κατεβάζει" από το διαδίκτυο.
Ποια περίπτωση ελέγχου της πρόσβασης θα έπρεπε να έχει εξασφαλιστεί για να ελαχιστοποιηθούν οι κίνδυνοι και γιατί;

Κ-5.2

16287.2. Ένα μικροβιολογικό εργαστήριο καταχωρίζει τα ιατρικά δεδομένα των πελατών – ασθενών σε ένα πληροφοριακό σύστημα που βρίσκεται εγκατεστημένο σε έναν υπολογιστή. Ο υπολογιστής αυτός βρίσκεται σε κοινόχρηστο χώρο, δεν προστατεύεται από κωδικό και είναι μόνιμα συνδεδεμένος με το Διαδίκτυο.
Εξηγήστε με συντομία τους λόγους για τους οποίους το παραπάνω πληροφοριακό σύστημα δεν ικανοποιεί τουλάχιστον δύο από τις βασικές αρχές ασφάλειας πληροφοριακών συστημάτων (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα).

Κ-5.2

16284.2. Η δημιουργία αντιγράφων ασφαλείας (backup) σε εξωτερικό δίσκο USB, μόνιμα συνδεδεμένο με τον υπολογιστή, δεν είναι καλή πρακτική. Εξηγήστε με συντομία τους λόγους.

Κ-5.2

16334.1 Για να ικανοποιηθούν οι απαιτήσεις ασφαλείας ενός Πληροφοριακού Συστήματος (Π.Σ.) και να μειωθεί η επικινδυνότητα σχεδιάζονται κάποια μέτρα ασφαλείας. Κατηγοριοποιήστε τα είδη των μέτρων ασφαλείας στην πρώτη στήλη Α, ανάλογα με τις κατηγορίες που αυτά καλύπτουν στην δεύτερη στήλη Κ .

Α. ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ	**Κ. ΚΑΤΗΓΟΡΙΕΣ**
Α1. Απογραφή λογισμικού και υλικού	Κ1. Διοικητικά μέτρα
Α2. Αντίγραφα ασφαλείας (backup)	Κ2. Τεχνικά μέτρα
Α3. Εκπαίδευση χρηστών για τις λειτουργίες του Π.Σ.	Κ3. Μέτρα φυσικής ασφάλειας
Α4. Διαβάθμιση πληροφοριών	
Α5. Αδιάλειπτη παροχή ρεύματος (UPS)	
Α6. Πρόσβαση στις κτιριακές εγκαταστάσεις	
Α7. Αρχεία καταγραφής (log files)	

Κ-5.2

20777.1 Αντιστοιχίστε τα ακόλουθα σενάρια δυνητικών απειλών κατά δεδομένων με τις Βασικές Αρχές Ασφάλειας Πληροφοριακών Συστημάτων που παραβιάζονται σε κάθε ένα από αυτά. Ας σημειωθεί ότι σε κάποια σενάρια μπορεί να παραβιάζονται περισσότερες από μία Βασικές Αρχές Ασφαλείας.

Σενάριο	Βασικές Αρχές
1. Εισβολή χάκερ στο μηχανογραφικό σύστημα μιας Πανεπιστημιακής σχολής, προβολή των βαθμολογιών των φοιτητών και αλλαγή κάποιων από αυτούς.	Α. Εμπιστευτικότητα
2. Κλείδωμα των αρχείων ενός χρήστη υπολογιστικού συστήματος με σκοπό την απαίτηση χρημάτων για το ξεκλείδωμά τους.	Β. Ακεραιότητα
3. Διαδικτυακή επίθεση σε server ηλεκτρονικού καταστήματος με συνέπεια τη διακοπή της λειτουργίας του για 48 ώρες.	Γ. Διαθεσιμότητα
4. Υποκλοπή των ιατρικών δεδομένων των ασθενών ενός νοσοκομείου.	
5. Εγκατάσταση κακόβουλου λογισμικού παρακολούθησης των ενεργειών των χρηστών ενός υπολογιστικού συστήματος	
6. Μεταβολή του περιεχομένου ενός μηνύματος ηλεκτρονικού ταχυδρομείου που αποστέλλει ένας χρήστης υπολογιστή.	
7. Εισαγωγή κακόβουλου λογισμικού σε υπολογιστικό σύστημα το οποίο ενσωματώνεται στα εκτελέσιμα αρχεία και καταγράφει τους κωδικούς που εισάγει ο χρήστης σε σελίδες στο Διαδίκτυο.	

Κ-5.2

21424.2 Να αντιστοιχίσετε τις ενέργειες της στήλης **Α** με τις διαδικασίες της στήλης **Β** με τις οποίες σχετίζονται στα πλαίσια της διαχείρισης ασφάλειας ενός πληροφοριακού συστήματος.

Α. ΕΝΕΡΓΕΙΑ	**Β. ΔΙΑΔΙΚΑΣΙΑ**
Α1. Αναγνώριση ευπαθειών	**Β1.** Διαχείριση Κινδύνου
Α2. Περιγραφή νομικών περιορισμών που διέπουν τη λειτουργία του οργανισμού	**Β2.** Πολιτική Ασφάλειας
Α3. Αναγνώριση απειλών	**Β3**. Σχέδιο Επαναφοράς από καταστροφή
Α4. Χαρακτηρισμός εμπιστευτικότητας πληροφοριών	
Α5. Δημιουργία αντιγράφων ασφαλείας	
Α6. Περιγραφή Στόχων ασφάλειας	
Α7. Δοκιμές επαναφοράς συστήματος από αντίγραφα ασφαλείας	

Κ-5.2

20786.2 Να αντιστοιχίσετε τα μέτρα υλοποίησης του Σχεδίου Ασφαλείας για το Πληροφοριακό Σύστημα ενός οργανισμού (στήλη Α) με την κατηγορία στην οποία ανήκουν (στήλη Β). Να γράψετε στο τετράδιό σας τον αριθμό του μέτρου και τον αριθμό της κατηγορίας στην οποία αντιστοιχεί.

Α. Μέτρο	**Β. Κατηγορία**
Α1. Περιγραφή ρόλων και αρμοδιοτήτων του προσωπικού ενός οργανισμού.	**Β1.** Διοικητικά μέτρα
Α2. Εγκατάσταση ισχυρών κλειδαριών στις εγκαταστάσεις των υπολογιστών	**Β2.** Τεχνικά μέτρα
Α3. Περιγραφή της διαβάθμισης των πληροφοριών	**Β3.** Μέτρα φυσικής ασφάλειας
Α4. Λήψη αντιγράφων ασφαλείας	
Α5. Ασφαλείς δοκιμές εφαρμογών λογισμικού	
Α6. Τοποθέτηση συσκευών αδιάλειπτης παροχής ρεύματος	

Κ-5.2

20030.2 Για κάθε ένα από τα σενάρια που περιγράφονται στη στήλη Α γράψτε την έννοια της Ασφάλειας Πληροφοριακών Συστημάτων της στήλης Β με την οποία αντιστοιχεί.

(Α)	**(Β)**
1. Κενό ασφαλείας στο Λειτουργικό Σύστημα Windows που επιτρέπει την απομακρυσμένη πρόσβαση με δικαιώματα διαχειριστή στο σύστημα.	Α. Απειλή
2. Πιθανό συμβάν διακοπής ρεύματος στο κέντρο μηχανογράφησης μιας επιχείρησης	Β. Ευπάθεια
3. Διαγραφή σημαντικών αρχείων λόγω λάθους χειρισμού από χρήστη υπολογιστή.	Γ. Αντίμετρα
4. Εγκατάσταση ενημέρωσης που διορθώνει κενά ασφαλείας στο Λειτουργικό Σύστημα Linux.	
5. Εγκατάσταση συστήματος πυρόσβεσης στο κέντρο μηχανογράφησης μιας επιχείρησης.	
6. Χρήση εύκολα προβλέψιμου κωδικού πρόσβασης από έναν χρήστη ενός υπολογιστικού συστήματος.	
7. Κλείδωμα των αρχείων ενός οργανισμού από επιτιθέμενο χάκερ και απαίτηση καταβολής χρηματικού ποσού για την επαναφορά τους.	
8. Διοργάνωση σεμιναρίου στους υπαλλήλους μια επιχείρησης σχετικά με τις επιθέσεις τύπου κοινωνικής μηχανικής.	
9. Εγκατάσταση προγράμματος ανίχνευσης και αντιμετώπισης ιών σε υπολογιστές.	
10. Παράλειψη εγκατάστασης των σημαντικών ενημερώσεων ασφαλείας ενός Λειτουργικού Συστήματος	

Κ-5.2

20063.2. Παρακάτω δίνονται κάποια παραδείγματα κακόβουλου λογισμικού. Ποιες από τις τρεις βασικές αρχές της ασφάλειας πληροφοριακών συστημάτων (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα) απειλούν;

1. Spyware
2. Adware
3. Botnet
4. Viruses

Να δικαιολογήσετε την απάντησή σας. Να ληφθεί υπόψιν ότι ένας τύπος κακόβουλου λογισμικού μπορεί να απειλήσει περισσότερες από μία αρχές.

Κ-5.2

20034.3 Για κάθε μία από τις απειλές που αναφέρονται στις παρακάτω προτάσεις προτείνετε ένα αντίμετρο που θα μπορούσε να χρησιμοποιηθεί για να την προλάβει ή να την αντιμετωπίσει.

1. Απώλεια των δεδομένων ενός σκληρού δίσκου λόγω μηχανικής βλάβης
2. Υποκλοπή ευαίσθητων προσωπικών δεδομένων από υπολογιστικό σύστημα, από επιτιθέμενο που εκμεταλλεύτηκε γνωστό κενό ασφαλείας του Λειτουργικού Συστήματος.
3. Συχνές διακοπές ρεύματος στην περιοχή που βρίσκεται το κέντρο μηχανογράφησης μιας επιχείρησης.
4. Εισαγωγή κακόβουλου λογισμικού σε υπολογιστικό σύστημα.
5. Διοίκηση και προσωπικό ενός οργανισμού που δεν γνωρίζει πως να αντιμετωπίσει μια περίπτωση παραβίασης ασφάλειας.

Κ-5.2

20053.1. Να χαρακτηρίσετε τις παρακάτω καταστάσεις στην στήλη Α ως Ευπάθειες ή Αντίμετρα επιλέγοντας την κατάλληλη κατηγορία από τη στήλη Β στον παρακάτω πίνακα. Κάποιες επιλογές της στήλης Α μπορεί να μην αντιστοιχούν σε κανέναν από τους δύο χαρακτηρισμούς:

Α. ΚΑΤΑΣΤΑΣΗ	**Β. ΧΑΡΑΚΤΗΡΙΣΜΟΣ**
Α1. Ύπαρξη μη ασφαλούς συνθηματικού (password)	**Β1.** Ευπάθεια
Α2. Καταστροφή από φυσικά φαινόμενα	**Β2.** Αντίμετρο
Α3. Η πρόσβαση στο δίκτυο δεν περιορίζεται	
Α4. Τακτική λήψη αντιγράφων ασφαλείας	
Α5. Εγκατάσταση λογισμικού antivirus	
Α6. Μη εγκατάσταση ενημερώσεων λειτουργικού συστήματος	
Α7. Σωστή ρύθμιση συστήματος ανίχνευσης εισβολής	
Α8. Επιθέσεις κοινωνικής μηχανικής	

Κ-5.2