



Νικόλαος Κολοκοτρώνης
Καθηγητής

Διάρκεια εξέτασης
2,5 ώρες

Ασφάλεια Συστημάτων

ΕΞΕΤΑΣΤΙΚΗ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2025

Θέμα 1ο (1.0 μονάδα)

Ποιο είναι το τρίπτυχο της ασφάλειας; Να περιγράψετε (λεπτομερώς):

- (α) Πιθανά παραδείγματα/τρόπους ενσωμάτωσης σχετικών μηχανισμών ασφάλειας σε λειτουργικά συστήματα (π.χ. Linux και Windows), και
- (β) Μια επίθεση για καθένα παράδειγμα μηχανισμού ασφάλειας.

Θέμα 2ο (2.0 μονάδες)

Εξηγήστε τον τρόπο που λειτουργεί η πιστοποίηση χρηστών μέσω συνθηματικών. Με ποιο μηχανισμό προστατεύονται τα συνθηματικά χρηστών στο Unix; (θεωρήστε ως παράδειγμα την υλοποίηση της `crypt(3)` συνάρτησης) Να παρουσιάσετε αναλυτικά δυο τεχνικές επιθέσεων ανάκτησης συνθηματικών καθώς και μέτρα προστασίας.

Θέμα 3ο (3.0 μονάδες)

Να περιγράψετε τη δομή, τη λειτουργία, και τον τρόπο που συνδέονται μεταξύ τους:

- (α) Τα ψηφιακά πιστοποιητικά X.509 (εξηγήστε και τους αναγκαίους ελέγχους που πραγματοποιούνται για να εμπιστευτούμε ένα πιστοποιητικό X.509).
- (β) Το πρότυπο των λιστών ανακληθέντων πιστοποιητικών CRL (εξηγήστε και τα θέματα που ανακύπτουν ως προς τη διαχείριση καθώς και προτάσεις επίλυσης)
- (γ) Το πρωτόκολλο OCSP λήψης της κατάστασης ενός ψηφιακού πιστοποιητικού X.509.

Θέμα 4ο (3.0 μονάδες)

Περιγράψτε τα ακόλουθα για το πρωτόκολλο SSL v3.0:

- (α) τα μηνύματα του SSL Handshake αναλυτικά,
- (β) τον τρόπο παραγωγής του master secret και του απαιτούμενου key material,
- (γ) τη διαμόρφωση του πρωτοκόλλου εάν το ψηφιακό πιστοποιητικό του server έχει ανακληθεί. Υπάρχει πρωτόκολλο που θα χειριστεί μια τέτοια περίπτωση;

Θέμα 5ο (1.0 μονάδα)

Τι είναι οι απομακρυσμένες ευπάθειες; Ποια η διαφορά του worm από το virus; Τι είναι η ευπάθεια μηδενικής ημέρας (zero-day vulnerability) και που χρησιμοποιείται;