Ερώτημα 1:

c. password : iNSeCuRe

Ποιο αποδοτική μέθοδος ήταν η επίθεση λεξικού διότι χρησιμοποιεί τις ήδη υπάρχουσες λέξεις προκειμένου να βρει το password το οποίο το καταφέρνει σε μερικά δευτερόλεπτα, σε αντίθεση με την μέθοδο brute force που χρειάζεται αρκετά μεγάλο χρονικό διάστημα

d. Μερικά μέτρα προστασίας του password είναι : συχνή αλλαγή του password, αποφυγή διατήρησης των password σε κάποιο αρχείο μέσα στον υπολογιστή, να μην γίνεται γνωστό το password σε τρίτους ακόμα και οικειοθελώς.

e. Η μορφή που πρέπει να έχει ένα password για να θεωρείται ασφαλές είναι : να μην ενσωματώνει “έτοιμες” λέξεις ή συνηθισμένες προκειμένου να αποφευχθούν επιθέσεις λεξικού. Επίσης συνιστάται η χρήση αρκετών χαρακτήρων ώστε πιθανή χρήση της μεθόδου brute force να χρειαστεί αρκετό καιρό μέχρι να τελειώσει με επιτυχία.

Ερώτημα 2:

a. Password = insecurity

Ερώτημα 3:

Root : toor

Test1 : test

Test2 : 123456

Test3 : qwerty

Οι απαντήσεις βρέθηκαν κάνοντας χρήση του εργαλείου john the ripper

b. Κάποια password δεν αποκαλύπτονται διότι είναι λέξεις που ήδη προϋπάρχουν σε λεξικό

c. Μια λύση είναι να μην επιτρέπεται η πρόσβαση στο αρχείο σε χρήστες που δεν είναι διαχειριστές