

ΘΕΜΑ 4

Μελετήστε το επόμενο κείμενο και απαντήστε στις ερωτήσεις που ακολουθούν:

Ένα rootkit είναι λογισμικό που όταν εγκατασταθεί σε έναν υπολογιστή επιτρέπει την πρόσβαση με δικαιώματα διαχειριστή σε μη εξουσιοδοτημένους χρήστες, συχνά αποκρύπτοντας τα αρχεία και τις διεργασίες που θα μπορούσαν να αποκαλύψουν την ύπαρξή του. Ο όρος προέρχεται από τη συνένωση των λέξεων «root» (το παραδοσιακό όνομα του λογαριασμού διαχειριστή σε συστήματα τύπου Unix) και «kit». Αν και τα rootkit δεν αποτελούν από μόνα τους απειλή, πολλές φορές χρησιμοποιούνται για να καλύπτουν άλλα κακόβουλα λογισμικά.

Η εγκατάσταση ενός rootkit μπορεί είτε να γίνει αυτόματα, χωρίς να το καταλάβει ο ιδιοκτήτης του υπολογιστή, ή από έναν επιτιθέμενο που θα το εγκαταστήσει αφού αποκτήσει πρόσβαση επιπέδου διαχειριστή λόγω κάποιας ευπάθειας του λειτουργικού συστήματος ή με την απόκτηση κάποιου κωδικού πρόσβασης.

Από τη στιγμή που το λογισμικό εγκαθίσταται έχει τη δυνατότητα να αποκρύπτει την εισβολή, διατηρώντας ταυτόχρονα πλήρη έλεγχο του συστήματος και με τον τρόπο αυτό να αποφεύγει τον εντοπισμό του από τα προγράμματα προστασίας. Η αφαίρεσή του μπορεί να είναι από πολύπλοκη έως πρακτικά αδύνατη, ειδικά αν αυτό έχει ενσωματωθεί στον πυρήνα του λειτουργικού συστήματος. Πολλές φορές η επανεγκατάσταση του λειτουργικού συστήματος μπορεί να είναι η μόνη λύση.

4.1 Για πιο λόγο τα rootkit είναι πιο δύσκολο να αντιμετωπισθούν, σε σχέση με τα υπόλοιπα είδη κακόβουλου λογισμικού;

Μονάδες 4

4.2 Αναφέρετε τρεις ενέργειες ενός χρήστη που χρησιμοποιεί το διαδίκτυο και θα μπορούσαν να οδηγήσουν στην εν αγνοία του εγκατάσταση rootkit στον υπολογιστή του.

Μονάδες 6

4.3 Αναφέρετε δύο αντίμετρα που θα μπορούσαν να αποτρέψουν την εγκατάσταση rootkit σε ένα υπολογιστικό σύστημα.

Μονάδες 6

4.4 Αναφέρετε τρεις (3) απειλές με τις οποίες θα μπορούσε να έρθει αντιμέτωπος ένας χρήστης ο υπολογιστής του οποίου βρίσκεται κάτω από τον πλήρη έλεγχο ενός rootkit.

Μονάδες 9