ΘΕΜΑ 4

Σε ένα δίκτυο μιας εταιρίας που παρέχει ηλεκτρονικές υπηρεσίες παρουσιάστηκε το εξής πρόβλημα ασφάλειας**.** Σε συγκεκριμένη χρονική στιγμή παρουσιάστηκαν ταυτόχρονα χιλιάδες απαιτήσεις εγγραφής από χρήστες στις υπηρεσίες της εταιρίας. Οι υπολογιστές που παρείχαν αυτή την υπηρεσία λόγω φόρτου κατέρρευσαν, και ο δικτυακός τόπος της εταιρίας έγινε μη λειτουργικός για μεγάλο διάστημα.

4.1 Να δώσετε την ονομασία στο είδος της επίθεσης που προκάλεσε το πρόβλημα ασφάλειας που ανιχνεύθηκε στην παραπάνω περίπτωση.

Μονάδες 3

ΑΠΑΝΤΗΣΗ:

Κυκλοφοριακή Πλημμύρα (Traffic Flooding)

4.2 Εξηγήστε πως λειτουργεί αυτή η περίπτωση παραβίασης και ποιος είναι ο πιο πιθανός λόγος πρόκλησης της;

Μονάδες 8

ΑΠΑΝΤΗΣΗ:

Αυτή η επίθεση είναι μια έξυπνη μέθοδος για την διείσδυση σε ένα δίκτυο η οποία απλά στοχεύει στα συστήματα ανίχνευσης εισβολής, δημιουργώντας πολύ μεγάλο φόρτο από κυκλοφορούντα πακέτα τα οποία το σύστημα αδυνατεί να παρακολουθήσει επαρκώς. Με αυτή την κυκλοφοριακή συμφόρηση οι επιτιθέμενοι στοχεύουν σε άρνηση υπηρεσίας (DoS).

4.3 Να αναφέρετε ποια από τα βασικά χαρακτηριστικά ασφάλειας (Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα) παραβιάζονται και τι σημαίνει αυτό ;

Μονάδες 8

ΑΠΑΝΤΗΣΗ:

Παραβιάζεται η Διαθεσιμότητα (Availability). Διαθεσιμότητα σημαίνει ότι οι υπολογιστές, τα δίκτυα, τα δεδομένα και γενικότερα οι υπολογιστικοί πόροι θα είναι στη διάθεση των εξουσιοδοτημένων χρηστών όποτε απαιτείται η χρήση τους. Η πιο συχνή απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι οι επιθέσεις άρνησης

υπηρεσιών (DOS attack), που έχουν ως σκοπό να τεθούν εκτός λειτουργίας συγκεκριμένοι υπολογιστικοί πόροι, είτε προσωρινά είτε μόνιμα

4.4 Για να συλλεχθούν πληροφορίες σχετικά με την περίπτωση που η παραβίαση έγινε από το εσωτερικό δίκτυο της εταιρίας, χρησιμοποιήθηκαν τα αρχεία καταγραφής. Εξηγήστε για ποιο λόγο χρησιμοποιήθηκαν, τι περιέχουν τα αρχεία αυτά;

Μονάδες 6

ΑΠΑΝΤΗΣΗ:

Τα αρχεία καταγραφής (log-files) περιέχουν πληροφορίες χρήσιμες για την παρακολούθηση της δραστηριότητας στο δίκτυο, όπως είναι χρόνος σύνδεσης, χρήστης, σταθμός εργασίας, αρχεία που έγινε πρόσβαση κλπ.