ΘΕΜΑ 4

4.1

Κυκλοφοριακή Πλημμύρα (Traffic Flooding)

4.2

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

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

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.