Σκοπός της εργαστηριακής άσκησης ήταν να εκμεταλευτούμε ευάλωτες ρουτίνες οι οποίες επέτρεπαν στον χρήστη να υπερχειλίσει την στοίβα με σκοπό να εισάγει δικό του κώδικα προς εκτέλεση.Στην περίπτωση μας είχαμε την vulnerable.c.Η ιδέα είναι να γεμίσουμε τον buffer έτσι ώστε να υπερχειλίση η στοίβα και να πάει να πανωγράψει σε ότι ακολουθεί και συγκεκριμένα να αλλάξει την διεύθυνση επιστροφής της καλούμενης στο σημείο όπου θα ξεκινάει το shellcode μας.Το σημείο στη μνήμη που θα επιστραφεί δεν είναι δεδομένο οπότε πρέπει να εισάγουμε Nop Sleds δηλαδή εντολές του επεξεργαστή οι οποίες δεν κάνουν τίποτα και περνουν την εκτέλεση στην επόμενη εντολή.Ο buffer είναι πίνακας 100 χαρακτήρων.Στην command του αρχείου exploit_vulnerable.c περνάμε το εκτελέσιμο της vulnerable.Το μέγεθος του εκτελέσιμου είναι 14 byte(έπειτα από χρήση της strlen).Τα περιεχόμενα της command θα είναι της μορφής ./vulnerable + Nops + shellcode(100 byte ίσο με το μέγεθος του buffer) + 100 byte (25 RET των 4 byte ) για την συμπλήρωση του command(όπου command[200]).Συνεπώς,έχουμε 14 byte για ./vulnerable,25 byte shellcode (25 hex σύμβολα του ενός byte) και ο buffer συμπλήρώνεται με 61 Nops.Το υπόλοιπο μισό της command περιλαμβάνει 25 RET στην διεύθυνση επιστροφής της καλούμενης όπου έχουμε εισάγει τον κώδικά μας.