1. Il programma in questione è un gioco, tramite alcuni comandi come “if/else”,l’utente scegli tra l’opzione A e l’opzione B, l’opzione A ci permette di giocare, il programma ci proporrà delle domande e alla fine del gioco, ti chiederà di iniziare una nuova partita premendo A, ricomincerà il gioco. Se si dovesse scegliere l’opzione B ti farà uscire dal gioco direttamente, senza giocare.
2. Se dovessimo prendere una scelta diversa scegliendo quindi un’ipotetica lettera C, il programma si arresterà, nel codice non è prevista una terza scelta, nemmeno nel diagramma a blocchi presente nelle slide, si avrà un ciclo infinito nella ricerca della variabile “C”, senza un esito, questo farà arrestare il programma.
3. Nel caso in cui il giocatore dovesse inserire un nome con più di 20 caratteri, si verificherà un “buffer overflow”, una vulnerabilità di sicurezza, creata involontariamente da un programmatore, questa si verifica quando un programma scrive dei dati (inseriti come stringhe) che finiscono al di là del loro spazio di memoria, questa condizione può creare un crash del programma e altri errori e può essere sfruttato dagli hacker “black hat” che frammentando codice malevole lo inseriscono (anche grazie all’ausilio dei puntatori), negli spazi di memoria successivi in cui sono sfociati i dati. Il blackhat potrebbe creare seri danni al programma, fortunatamente per i dispositivi di nuova generazione, il problema del buffer overflow è diminuito drasticamente (quasi nullo), ed è un problema legato a programmi in cui si è utilizzato il linguaggio C per programmare.