1- *Buffer Overflow*

Pergunta 1.1

- **Java**: Ao executar o programa em Java acontece a exceção "*ArrayIndexOutOfBoundsException*".
- **Python**: Ao executar o mesmo programa em Python acontece que se inserirmos mais de 10 números, ele dá erro "*index out of range*", o que faz com que ele não consiga inserir mais números.
- **C++**: Ao executar em C++ o programa executa sem dar exceção.

Pergunta 1.2

- **Java**: Ao executar o programa em Java acontece a exceção "*ArrayIndexOutOfBoundsException*".
- **Python**: Ao executar o mesmo programa em Python acontece que ao inserirmos o décimo número o ciclo pará o que faz com que dê o erro "*index out of range*".
- **C++**: Ao executar em C++ o programa simplesmente não termina.

Pergunta 1.3

- **RootExploit.c**: Como neste programa são usados gets, então passando o tamanho do buffer este continua a escrever em memória, desta forma vai alterando a variável que atribui as permissões, mesmo a password estando errada.
- **0-simple.c**: Neste programa se escrevermos mais de 64 caracteres, vamos estar a escrever na variável *control*, pela mesma razão que a indicada no programa anterior.

Pergunta 1.4

Podemos concluir que este programa imprime parte dos caracteres inseridos. Este parte é do tamanho indicado antes. Caso o número de caracteres ditos como tamanho seja superior a 100 e os inseridos também, então o programa não imprime nada.

Pergunta 1.5

Para explorar esta vulnerabilidade foram inseridos 16 caracteres e depois 'dcba'. Desta forma, passa para o buffer[64], o strcpy não confirma tamanhos.

Pergunta 1.6

Pergunta 1.7