Level 1
Передать любую строку, длина которой больше 127, т.к. произойдет переполнение char’a

Level 2
Передать 4294967292 2 2, т.к если к 4294967292 прибавить 4, то uint станет равным 0

Level 3
Передать отрицательное число, т.к. uint обернется по модулю => uint будет больше 200

Level 4
Передать 4294967294, т.к. при добавлении 2 в uint будет 0

Level 5
Передать больше 15 символов (код символа 16 не равен 5), чтобы символ 16 символ записался в следующую ячейку памяти, где находится a.

Level 6
Передать System32, где находится cmd.exe

Level 7
Передать 16 любых символов, чтобы получилось переполнение. Это изменит младший байт в b

Level 8
Передать "%x %x %x"
prinf подставляет в этот формат три следующих своих аргумента. printf находит аргументы на стеке, где будут адрес возврата, адрес строки формата и переменная i, т.к. ничего не было передано.

Level 9
Передать 11111 11111111111111111111111111111111

Размер key 32 + 5. Туда копируется “key=” и пароль из 32 символов. Итого 38 символов (+2 для окончания строки) => в i записывается последний символ пароля

Level 10

Ничего не передавать.
В argv[0] находится путь к исполняемому файлу. В нём отсутствуют нулевые байты, и его длина больше 16. После цикла значение i становится равно 16, 0 запишется в buf[16], где находится i.

Level 11

Передать любые 84 символа и DCBA.
В бинарном виде 0x41424344 это 01000001 01000010 01000011 01000100.
На стеке: eip - 4 байта, ebp - 4 байта, buf – 80 байт. Если передать строку из 88 байт, то первые 80 скопируются в buf, следующие 4 байта в ebp, а последние 4 байта в eip.
Если перевести каждый блок бинарного числа в символы, то получится ABCD. Но так как в стеке число лежит от младшего байта к старшему, то нужно вводить DCBA

Level 12

Передать любые 84 символа и ctrl+O ctrl+P @ ctrl+@.
При запуске уровня адрес функции unreachable. Если перевести его в двоичную систему, потом разбить на блоки по 8 бит и каждый блок перевести в десятичное число, то получатся коды символов 0, 64, 16 и 15. По таблице ASCII эти символы равны null, @, ^P, ^O соответственно. Эти байты в обратном порядке нужно записать в адрес возврата main, чтобы после выхода из неё была вызвана функция unreachable.
На стеке: buf – 80 байт, аргументы main – 4 байта, адрес возврата - 4 байта.