Question Set 0x08

HQS Challenge

January 21, 2016

The following questions are in 64-bit architecture.
To answer the following questions download this binary: chal0x01 or `https://goo.gl/ItW840`

1. What is the command to view the header of this program?

2. What is listed as the 'Entry Point address' for this program?

3. Is this programs stack listed as executable?

For the following questions download this binary: chal0x02 or `https://goo.gl/PW5Nnc`

1. What is the 'Entry point address'?

2. How many section headers are there in this binary?

3. How large are each of the section headers?

4. Forward thinking: Does the entry address match the address of the first function you expect to be called - probably main? Why?

5. Forward thinking: Why would it be beneficial to an attacker for the GNU_STACK to be listed as 'RWE'?

Solutions

1. `readelf -h chal0x01`

2. `0x4005b0`

3. No `GNU_STACK ... RW`

1. 0x4004b0

2. 30

3. 64 bytes

4. No, because the first thing to execute is not actually main, it is ‘_start’

5. That means that the stack is executable and hence, shellcode can be written directly onto the stack. A non-executable stack is commonly refered to as ‘NX’