CSAW RECAP


たまご


NYU
TANDON SCHOOL
OF ENGINEERING
6
METROTECH

PWN

```
joseph@ubuntu:~/Desktop/csaw19$ ./arevenge
```

```
joseph@ubuntu:~/Desktop/csaw19$ ./arevenge
X
ok, byebye!
joseph@ubuntu:~/Desktop/csaw19$
```

```
joseph@ubuntu:~/Desktop/csaw19$ ./arevenge
1
0
You found a secret!
```

```
int go() {
  uint8_t secret[] = {0xde, 0xad, 0xbe, 0xef, 0xca, 0xfe, 0xba, 0xbe};
  int choice;

  while (true) {
    cin >> choice;

    switch (choice) {
    case 1: // leak
      A(std::begin(secret));
      break;
    case 2: // write
      B(std::begin(secret));
      break;
    case 5: // exit
    default:
      cout << "ok, byebye!" << endl;
      return 0;
    }
  }
}
```

Checks input against ‘secret’

But, we decide how much input to test...

```
template <typename T> void A(T secret) {
  size_t size;

  cin >> size;
  std::vector<uint8_t> data = get(size);

  bool eq = std::equal(data.begin(), data.end(), secret);
  if (eq) {
    cout << "You found a secret!" << endl;
  } else {
    cout << "You didn't find a secret :(" << endl;
  }
}
```

We can write into the ‘secret’

But, we decide how much to write...

```
template <typename T> void B(T secret) {
  size_t size;
  cin >> size;

  std::vector<uint8_t> data = get(size);

  std::copy(data.begin(), data.end(), secret);
}
```

THE STACK

It’s where things go™

“SECRET” (0xdeadbeefcafebabe)
Random “Canary”
Return Address!
Bunch of 0x0A bytes
Another Canary
Address of LIBC
...

THE STACK

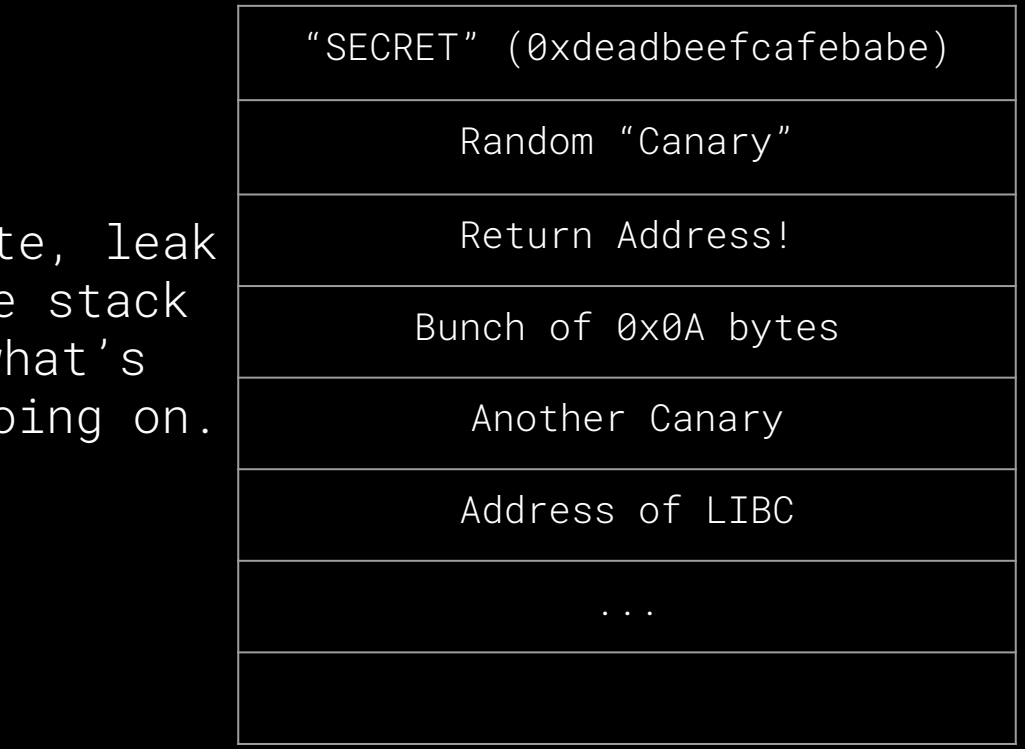
It's where things go™

We can make guesses about "Secret," and know if we are right...

THE STACK

It's where things go™

Byte by byte, leak the entire stack to see what's actually going on.



THE STACK

It’s where things go™

Once we know the canary value, we can overwrite return address with ROP + ret2libc