Baby Binary Workshop

Ashley Bilbrey

Quick Disclaimer

This workshop will be one of the more difficult this quarter.

Why?

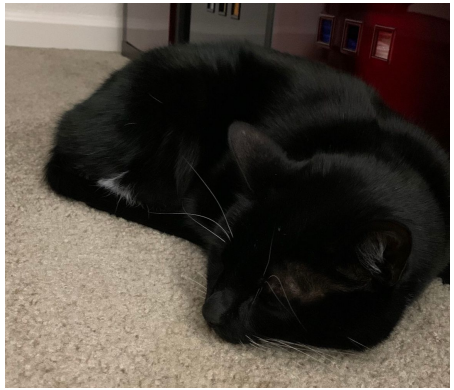
- Coding Knowledge
- Linux Knowledge
- Some Assembly Knowledge

But don’t worry too much! I tried to gear this towards a beginner audience.

Baby Binary?

What do I mean by Baby Binary?

Baby: Common CTF term - meaning easy, simple, beginner…
Binary: Most people think of binary as a numbering system or zeroes and ones. In this case, I mean an executable file.



Jeff (Baby)

```
01101000 01110100 01110100 01110000 01110011 00111010 00101111
00101111 01110111 01110111 01110111 00101110 01111001 01101111 01110101 01110100 01110101
01100010 01100101 00101110 01100011 01101111 01101101 00101111 01110111 01100001 01110100
01100011 01101000 00111111 01110110 00111101 01101001 01101001 01101011 00110010 00110101
01110111 01110001 01001001 01110101 01000110 01101111
```

Three Categories Today

- Overflows (Integer, Buffer)
  - “Binary Exploitation”
- Simple Binary “Poking” Techniques
- Reverse Engineering
  - Sort of a separate category from binary exploitation, but it’s semi-related and fun enough.

Integer Overflow

We'll start with this because it's simpler to conceptualize.

Imagine counting on your fingers. What do you do when you run out of fingers?

On computers, it can overflow.

··· -> 1100 -> 1101 -> 1110 -> 1111 -> 0000!!

Too Peaceful

+

Nuclear Gandhi in *Civilization*, too peaceful and would cause overflow. Urban legend? [Read More]

Challenge: PokeShop Shop

Download
https://daviscybersec.org/babybin/pokeshop

You can run the binary in terminal by running *./pokeshop*

Consider what we've learned so far. Can you think of a way to get the GS PokeBall?

Solution

Buy poffins!

The developer of this code forgot to implement checking if a customer had enough money to buy poffins. By buying more poffins than you can afford, you trigger an overflow and get a ton of money!

Buffer Overflow Concept

On a more conceptual level:

Buffer overflow is when user data is entered that is larger than a buffer, which causes the data to go into the next segment of memory. It’s a bit more complicated in practice.

What is your name?: Ashleyyyyyyyyyyaaaaaaaaaaaaa9999999999

Name	Balance

Strings

Poking Technique #1:
Often times flags and other useful information are hidden inside files. Often these are obfuscated, but sometimes they are not.

Use *strings <filename>* to display all strings in a binary.

Can you find the flag in the pokeshop binary?
Format ucd{...}

Examining Memory With GDB

Poking Technique #2:
GDB is a debugger tool. It's also useful for looking at memory!

Download https://daviscybersec.org/babybin/pokeshopcode.c

Use *gdb ./pokeshop*
Type *b main*, then type *start*

You can use *p <variablename>* to print a variable. Can you figure out how to print balance? Change it?

Reverse Engineering

Reverse engineering isn't really binary exploitation, but it can have similar mental process and is common in CTFs, so I thought to include it.

Reverse engineering problems often give a flag checker program that has the solution obfuscated. It requires some code know-how to figure out a solution. (Or sometimes force…)

Reverse Engineering Challenge

Download the Gym Badge Validator script from
https://daviscybersec.org/babybin/badgevalid.c

Can you find a valid Gym Badge Number?

Work with your neighbors for a solution!