High vs low level through a red team lens

Jarrett Lane

What does high/low level mean

- If we are talking about one thing, we can refer to it many ways
- We can refer to it in a general/high level sense, or a literal low-level sense.
- For Example: Coffee is a beverage, coffee is a liquid, coffee is a ton of atoms and molecules coming together in a certain way
- A beverage is a more general high-level idea, atoms are more specific and low level

Usage vs what it is

- When talking about something, we can also refer to it based off of what it is, or what it is used for
- For Example: A keyboard is a keyboard, input device, a computer accessory, and a machine
- We use a keyboard to type and send signals representing a character to the computer
- What are those signals? Electricity? 1s & 0s? Characters?

Abstraction

- Using a general idea to refer to something more complex/literal
- Not Just computers, but every day life
- Why is a 20$ bill worth 20$ if it is just Linen and cotton?
- When you make a call are you talking to a person or are you talking to the phone?

Why this matters with computers

- Lets take the letter é

- What if I told you é in binary is 11000011 10101001

- What if I told you its also 00000000 11101001

- This is because I am using two different ways to encode the letter

- Can this lead to a vulnerability? Yes

Note

- Before talking high vs low, it's important to understand that it's more of a spectrum
- It's not always high vs low level

Programs high vs low level

- On a high level, we know the computer just executes the code we give it and that’s it, the program will run how we intend for it to run
- On a low level it’s a bit more complicated, the program will run how the computer intends for it to run
- When you run code, the computer doesn't see what you wrote, it sees a ton of instructions that do what you wrote
- Compiling code is when you take human readable code and translate it to machine readable code
- The file containing this machine readable code is called an executable

High vs low level programming languages

- Programming languages can be high or low level
- High level languages like JavaScript or Python are flexible and easy to read
- Low level languages like C or Assembly are fast and offer more hardware management
- Each have their own benefits
- High level languages are better for software, low level languages are better for electronics

High level vulnerabilities

- High level vulnerabilities include:
  - unsafe design
  - unsafe configurations
  - logical loopholes
  - too much trust for a user
  - unexpected logic
  - etc

- High level is human error

Low level vulnerabilities

- Low level vulnerabilities include:
    - inconsistent interpretation of data
    - too much access to a programs memory
    - uncontrolled access to resources
    - etc.

- Low level is computer error

High or low level vulnerability?

- A server does not encrypt traffic
- Large input into a program overwrites the program's memory
- A user changes their session cookie and is now in another users account
- When handling numbers, a program takes a negative number and treats it as a huge positive number
- An attacker can interact with a database with customized queries
- An attacker can predict where sensitive data is stored in a programs memory

Interpretation

Data can be interpreted in many different ways by software

alert(1) in JavaScript is the same as: [][(![]+[])[+!+[]]+(!![]+[])[+[]] (the actual thing is 1000 characters I'm not pasting the whole thing)

Hello 0x00 World in C is the same as Hello

7+1 = -7

Weird behavior like this causes vulnerabilities

Sometimes, for functionality, data is evaluated and executed, what if that data is a malicious payload

This is both a high and low level issue

What I want you to understand

- What is 1s and 0s is an entire complex system
- Understanding how something on a computer runs on all levels is how you gain a deeper understanding
- In red team, hacking is using a system's or program's own logic against it, you have to understand that logic, at all levels
- See through the perspective of the computer, application, developer, and more
- Looking at something in different layers will help you understand a concept much faster

Interactive

- I made a challenge
- Go to the discord to access the challenge
- Hints:
    - What does eval() do?
    - Can you somehow make a function call?
    - There is more than one way to solve this
    - What are global variables?
    - How can you represent the string flag?
- If you have trouble reading code I will walk you through