CSE 351

Buffer Overflows and Lab3
Bufbomb Introduction

• Several stages
• Practice analyzing stack organization
• Practice with buffer overflows
Bufbomb Introduction

• GDB commands
  • set args -u <username>
    • Set the argument to the program
  • x/40wx ($rsp - 40)
    • Show the 40 bytes above rsp
    • Change w to g to check the value in 8 byte chunks.
  • b *(&getbuf + 12)
    • Create a breakpoint at 12 bytes away after the start of getbuf
Lab 3: Buffer Overflow

This has a buffer overflow

```c
int getbuf() {
    char buf[36];
    Gets(buf);
    return 1;
}
```

Why?
- `Get()` doesn't check the length of the buffer

The Stack in `getbuf()`

- `return addr`
- `saved regs (if any)`
- `local vars`
Lab 3: Buffer Overflow

This has a buffer overflow

```c
int getbuf() {
    char buf[36];
    Gets(buf);
    return 1;
}
```

Why?
- `Gets()` doesn’t check the length of the buffer

The Stack in `getbuf()`
- `return addr`
- `saved regs (if any)`
- `local vars`
Lab 3: Buffer Overflow

This has a buffer overflow

```c
int getbuf() {
    char buf[36];
    Gets(buf);
    return 1;
}
```

Why?
- `Gets()` doesn’t check the length of the buffer

The Stack in `getbuf()`

```
<p>| return addr |</p>
<table>
<thead>
<tr>
<th>saved regs (if any)</th>
</tr>
</thead>
<tbody>
<tr>
<td>buf [35]</td>
</tr>
<tr>
<td>buf [0]</td>
</tr>
</tbody>
</table>
```
Level 0: Call smoke()

Goal: call the smoke() function from getbuf()

```c
int getbuf() {
    char buf[36];
    Gets(buf);
    return 1;
}
```

How?
- overwrite the return address so we “return” to smoke()