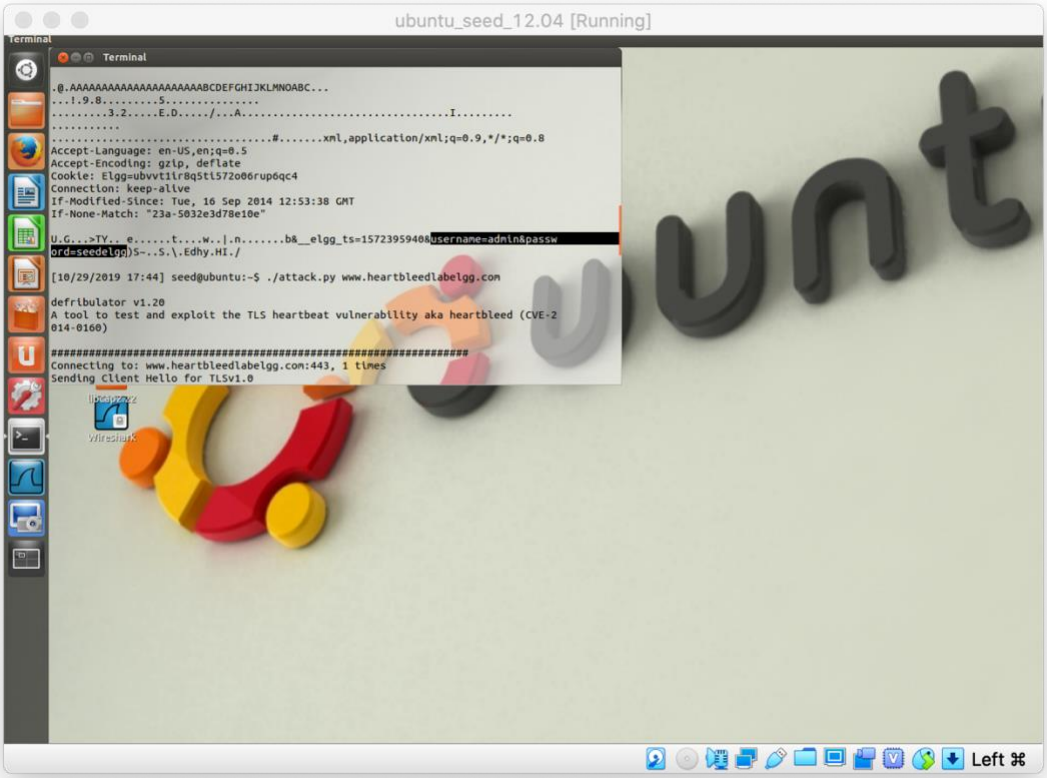
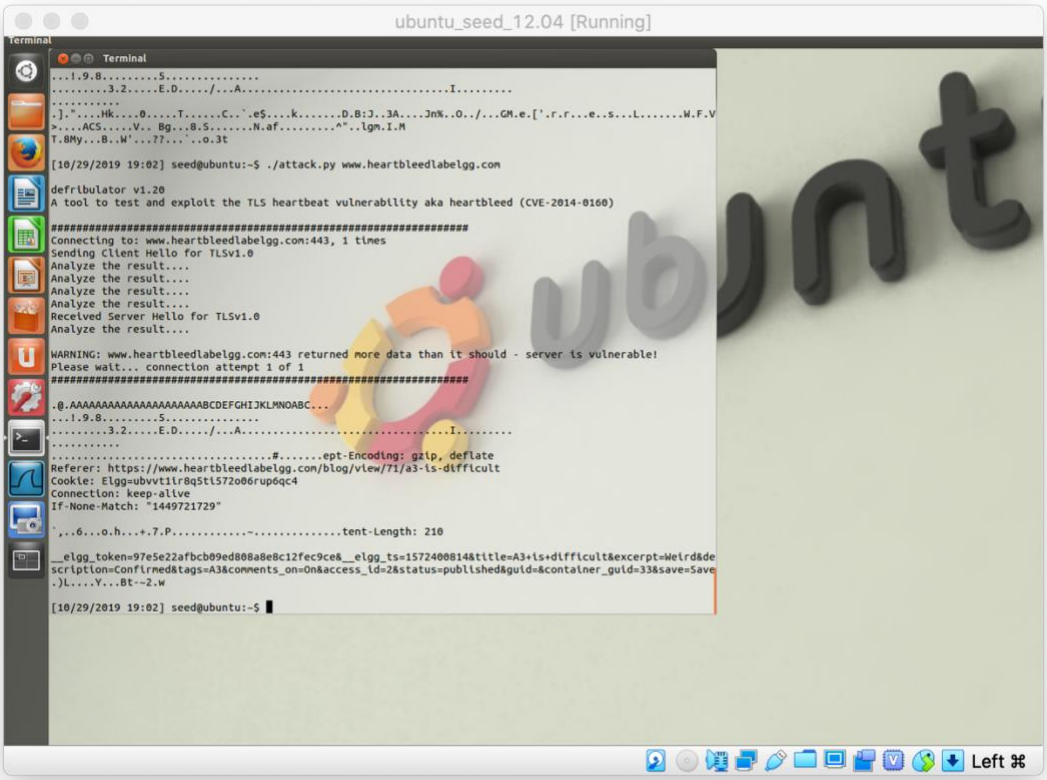


Username and Password

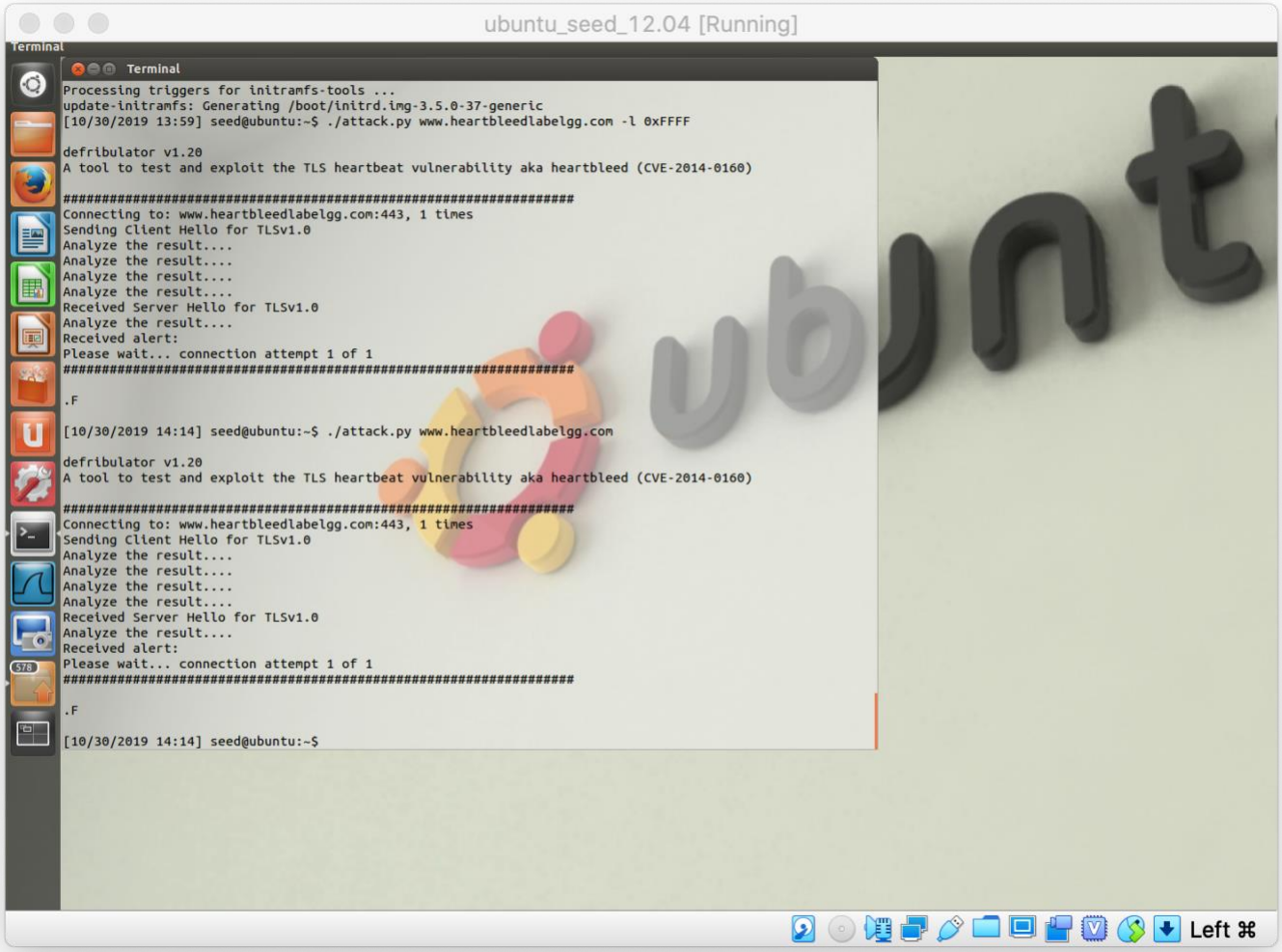


Activity: made a blog post titled “A3 is difficult” and found it using the attack

2.1
As the length variable decreases, so does the length of the output. I first started out with the length 0xFFFF. From there I went to 0x0FFF -> 0x00FF -> 0x000F -> 0x0001. As I decreased the length variable, the output decreased. The last two lengths 0x000F and 0x0001 yield practically the same output.

2.2
A boundary length of 22 results in a packet without any extra data.

3.1



3.2

```
memcpy(bp, pl, payload);
```

This piece of code does not conduct a check for `pl`. This problem could allow for a memory breach.

Solution:

```
// Server needs to calculate the packet size at runtime.
bool packetSize(packet) {
     // compare to see if the packet size is indeed correct
}

// if the packet size is correct, run the rest of the program
if (packetSize()) {
     // continue
} else {
     // error
}

memcpy(bp, pl, payload);
```

The new code should be place before the `memcpy` function is executed.