

**SI430: Lab 06 --- Packet Spoofing**

Names: **­ Brendan Lewis, Ian Coffey**

Alphas: 261194, 263708

External source(s)

Honor

We wrote the code on our own except the help from the external source(s) listed above. Moreover, we didn’t copy any part of the code from other midshipmen.

Initials: BAL & IKC

Challenges

The biggest challenged we face was constructing the packet correctly. It proved very difficult to debug and turns out most of our problems could be fixed with one line of code. Identifying that one line of code that needed to be corrected was far more difficult.

What we learned and what was interesting to us

We gained a fair amount of insight into the structure of a TCP packet and the in depth specifics of the sizes of certain parts of a TCP header. We thought it was interesting how a TCP packet is ultimately just a bunch of bytes strung together in a certain order, and anyone can perform packet spoofing.

# **Part 1:**

# 

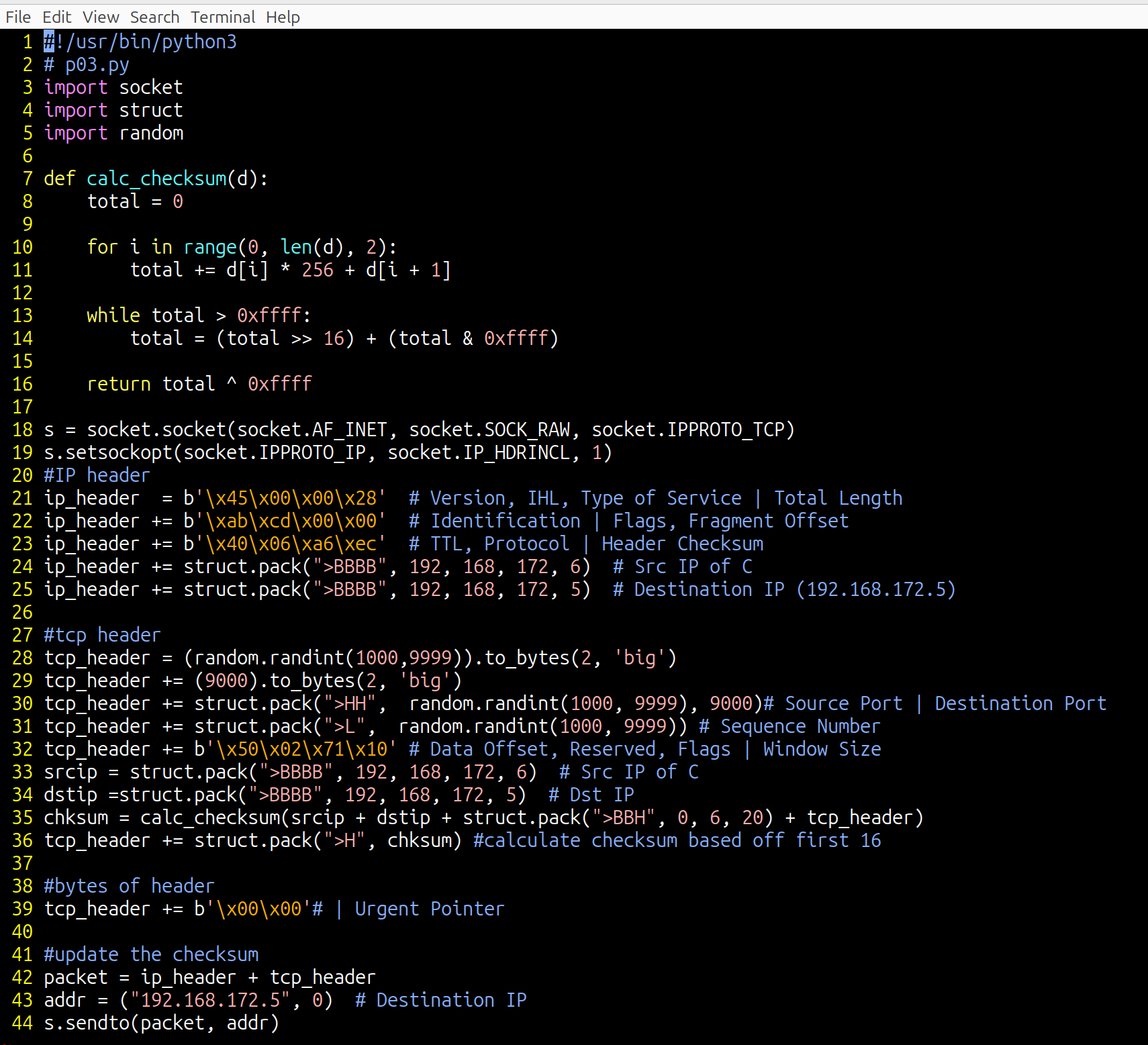
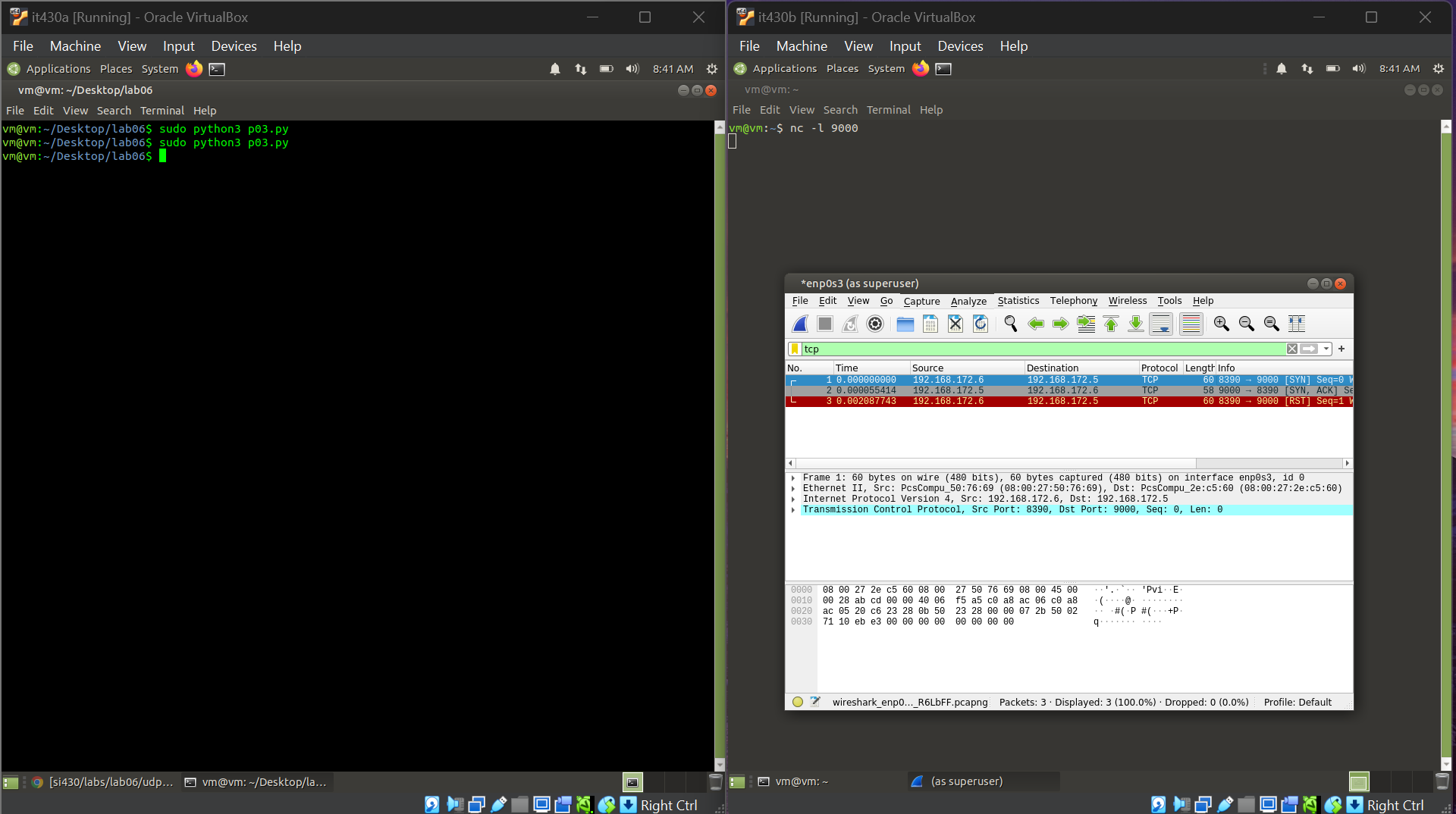
Part 1 of our lab is a simple udp packet constructed in python with the payload “hello world”. Looking at the code, there is a lot more in a udp packet than one would think, which made this decently difficult to do, but once we got over the learning curve, it was not too bad. After the udp packet was made, we sent it to another vm via a net cat connection. And as seen in the screenshot, it worked.

# **Part 2:**

# 

In part 2, we sent a syn packet to our vm. Our code builds upon what we did in part 1, but instead of sending a udp packet, we send a tcp packet with an associated ip header as well. So we had to manually construct an ip header and then add on a tcp header afterwards. Since this is a syn packet, we should receive a “syn ack” packet and an “ack” packet in wire-shark, which we did, so we know this code works.

# **Part 3:**



Part 3 is almost completely identical to part 2, however the only difference is that we were able to spoof the source address of our packet. So our packet says it is coming from 192.168.172.6, which is si430c. But in reality, the packet came from si430a, which is 192.168.172.4. This difference comes in the ip header, where we simply packed different bytes in order to fake the ip address. We did not even have to change the tcp header at all.