Snort Rule for Slammer

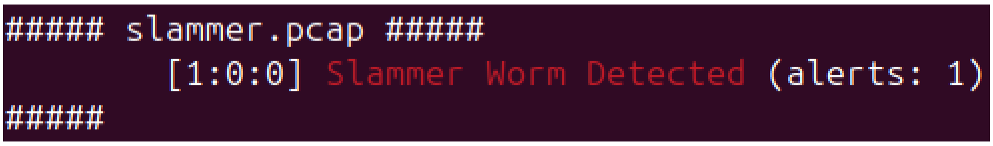
- alert udp 213.76.212.22 20199 -> 65.165.167.86 1434 (msg:"Slammer Worm Detected";)

Opening the pcap file with Wireshark we can see the following information about the packet:

- ➔ Source IP: 213.76.212.22
- ➔ Source Port: 20199
- ➔ Destination IP: 65.165.167.86
- ➔ Destination Port: 1434

So we create a rule that matches the specific characteristics of the packet to detect Slammer worm activity.

Screenshot:



```
##### slammer.pcap #####
        [1:0:0] Slammer Worm Detected (alerts: 1)
#####
```