Homework 3

1) Consider a company with two public production services (web and e-mail), with *standard* employees and employees with an access to a private sensitive database service. Design a network environment for this company. Show a diagram and describe how you'd configure network devices. Support your design decisions by security principles.

2) Run the following server. Can you crash it by sending packet(s) to it? If so, please demonstrate it and propose how to fix it. What would be implications if UDP was replaced by TCP?

```
import socket

UDP_IP = "127.0.0.1"
UDP_PORT = 5005

if __name__ == "__main__":
    sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
    sock.bind((UDP_IP, UDP_PORT))

    sizes = {}
    for size in range(512):
        sizes[size] = 0

    while True:
        data, addr = sock.recvfrom(8092)
        if addr[0] != "1.2.3.4": # on some systems should be addr != …
            print("Access denied")
            continue
        print "length:", len(data)
        sizes[len(data)] += 1
```

3) Implement a deep-packet inspector, that for all outgoing UDP packets prints a packet's payload only if it contains your group name and rejects such packets from being sent.
You can use packages like scapy and techniques like nfqueue (Netfilter queues) and TUN/TAP devices.