

## **Recitation 7: Group exercises**

1.Private Networks

2.Network Security

## 1. Private Networks

- What is the difference between an *intranet* and an *extranet*?
- What is a virtual private network (VPN)? How it is implemented?
- Describe network address translation (NAT). How it can be implemented in Linux?
- How can telnet sessions be blocked by a NAT?
- What is a demilitarized zone (DMZ)? What is it used for?

## 2. Network Security

- What is DIAMETER?
- What identifies a security association in IPSec?
- Is it better to use DES or Triple DES for ESP? Justify your choice?
- Why should the Security Association be changed after some time?
- Why was Postfix introduced?
- What are the advantages of xinetd over inetd?
- What is a hash function?
- What is a nonce? When it is used?
- What is a Diffie-Hellman key exchange? Why is it useful?
- Describe the Man-in-the-middle attack.
- What is a key distribution center (KDC)? Compare its different implementation approaches.
- Why was X.509 introduced?
- Compare Kerberos version 4 and 5.
- What are the different protocols used in Transport Layer Security (TLS)?
- Which application uses Pretty Good Privacy (PGP)? How it is deployed on the sender and receiver sides?