Exercises Lectures 1-4

Basic Network Security Terminology

1. What is the difference between security policy and security mechanism

2. Name 3 different kinds of security policies

3. Explain the following kinds of mechanisms: deter, deny, detect, delay and defend

4. Explain the following kinds of attacks: jamming, spoofing, hijacking, sniffing and poisoning.

5. Describe the functions of the transport, network and link layers in the network stack.

Network Attacks

1. Briefly explain how smurf attacks work

2. Explain the function of ARP and RARP, why ARP results are cached, and show how this can be used to spoof other computers.

3. What are SYN flood attacks? How can IP spoofing be used to make them more effective?

4. Discuss the advantages and limitations of on-path adversaries over off-path adversaries

5. Explain how TCP connections are setup through a 3-way handshake, and discuss TCP session hijacking by an on-path adversary.

6. Explain BGP sub prefix Hijacking

7. Explain how recursive DNS queries work and how this can be exploited to poison caches