Course: Security Engineering
Lecturer: Bruno Crispo

Written Exam: 26/02/2010
Questions should be answered in English.

Question 1 [1 point] (For all students)

1. Describe in detail what is a dictionary attack and how does it work?
2. Propose and explain in detail a solution that
    a. limits online dictionary attacks against a login protocol based on password
    b. does not allow denial-of-service against legitimate users

Question 2 [1 point] (For all students)

A bank wants to implement an online Internet banking service to allow its customers to consult (read) their monthly statements. The customers want to be sure to connect to their bank and want to keep all their information private (each customer must share her data only with the bank). The bank wants to allow only her customers to connect to this service. Please describe in detail all cryptographic technology and security protocols needed to implement such service and how they are used.

Question 3 [1 point] (Only for students that scored 0 points to assignment 1 or did not submit answers to assignment 1)

Describe the different alternatives to treat the risk identified during the evaluation phase?

Question 4 [1 point] (Only for students that scored 0 or 1 point to assignment 1 or did not submit answers to assignment 1)

Describe all the steps of a risk assessment methodology?

Question 5 [1 point] (Only for students that scored 0 points to assignment 2 or did not submit answers to assignment 2)

Why the need of a timestamp authority instead of letting users to timestamp their own signatures?

Question 6 [1 point] (Only for students that scored 0 or 1 point to assignment 2 or did not submit answers to assignment 2)

A certification authority cannot decrypt the messages sent by the users it certifies (for which it issues digital certificates). However which attack a fraudulent certification authority could still mount against the users it certifies?

Question 7 [1 point] (Only for students that scored 0 points to assignment 3 or did not submit answers to assignment 3)

Explain the effect of the following rules for the ACL of a packet filtering firewall

action	source	port	dest	port	flags
allow	120.46.66.xxx	*	154.60.98.xxx	*	
deny	120.46.66.176	*	178.67.98.90	80	
deny	*	*	156.39.100.54	>1024	

Question 8 [1 point] (Only for students that scored 0 or 1 point to assignment 3 or did not submit answers to assignment 3)

Write the rules that allow all the computers on the subnet 145.1.1.xxx to connect by means of ftp to the ftp server at the address 120.0.0.9

Question 9 [1 point] (Only for students that scored 0 points to assignment 4 or did not submit answers to assignment 4)

1. Explain in detail what are the differences between signature-based and anomaly-based intrusion detection systems.
2. Explain what are the advantages and the main problems of each of the previous techniques.
3. Explain what are the differences between an host-based and a network-based sensor.

Question 10 [1 point] (Only for students that scored 0 or 1 point to assignment 4 or did not submit answers to assignment 4)

Explain in detail what is a reflection attack.