Course: Security Engineering
Lecturer: Bruno Crispo

Written Exam: 02/02/2012
Questions should be answered in English.. It's a closed book exam.

Question 1 [1 point] (For all students)

1. Explain in detail what is the difference between signature-based and anomaly based intrusion detection systems.
2. Explain what are the advantages and the main problems of each technique.
3. Explain what is the difference between a host-based and a network-based sensor
4. Which type of IDS and sensor would you use to detect a buffer overflow and why.

Question 2 [1 point] (For all students)

Suppose there is a PKI that issues digital certificate upon request. Users use this PKI to get digital certificates needed to run cryptographic protocols allowing them to communicate securely. Unfortunately, this PKI does not implement revocation services and it's the only available PKI. Revocation however can be a problem for the users. Can still users use the digital certificates issued by such a PKI to communicate securely? If yes how this digital certificates should be?

Question 3 [1 point] (For all students)

1. Describe in detail why the 2nd per-image resistance property of cryptographic hash function is important and provide an example of its use
2. What is the collision resistance property of a cryptographic hash function?

Question 4 [1 point] (For all students)

Why when a digital certificate expires, the private key(signing key) corresponding to the public key included in the expired certificate needs to be deleted while the public key itself may need to be kept and used in the future?

Question 5 [1 point] (For all students)

1. What is the assurance of a security product?
2. Describe what are the requirements for a product to be certified EAL 4?

Question 6 (Only for students that scored 0 points to assignment 1 or did not submit answers to assignment 1)

Describe what are the different types of risk analysis a company may choose to carry out. Describe advantaged and disadvantages for each of them.

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

1. What are the different strategies companies can adopt to address the identified risk?
2. Give an example of operational control, one of technical control and one of management control.

Question 8 [1 point] (Only for students that scored 0 point to assignment 2 or did not submit answers to assignment 2)

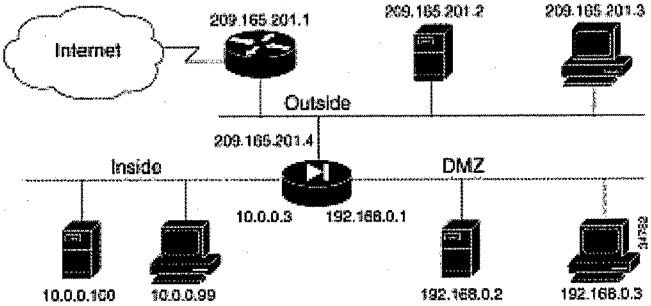
Please illustrate all the steps need to be executed by two parties (sender and receiver) to complete a transaction that cannot be later repudiated by any of the two parties. Clearly specify the steps for each party.

Question 9 [1 point] (Only for students that scored 0 or 1 point to assignment 2 or did not submit answers to assignment 2)

1. Give a specific example of application or scenario using SSL where it's enough to have server authentication only.
2. Give a specific example of application or scenario using SSL where it's necessary to have mutual authentication of both client and server.

Question 10 [1 point] (Only for students that scored 0 point to assignment 3 or did not submit answers to assignment 3)

Given the following network configuration, write the rules for the firewall (209.165.201.4) to allow any traffic coming only from 209.165.201.3 to access the internal machine 10.0.0.99 and for the machine 209.165.201.2 to access only the web server running on machine 192.168.0.2 . Furthermore, write the rule that allow only the machine 209.165.201.2 to access the telnet service running on the machine 10.0.0.99.


Internet
209.165.201.1
209.165.201.2
209.165.201.3
Outside
209.165.201.4
Inside
DMZ
10.0.0.3
192.168.0.1
10.0.0.100
10.0.0.99
192.168.0.2
192.168.0.3