Cairo
University

Faculty of Computers
and Information

Network Security
CS 495
2nd Term 2008-2009

Mid-term Exam #2 – Version A
[20 points + 3 points bonus]

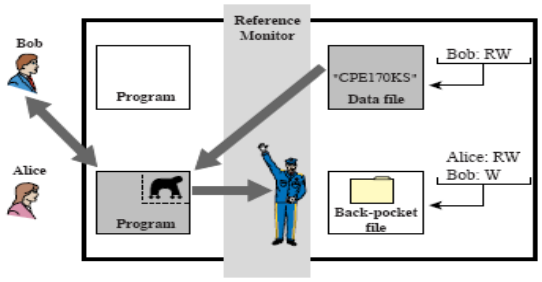
1. POP3 is an email exchange protocol. A POP3 server accepts connections at TCP port 110. Secure Shell (SSH) protocol is used to create a secure tunnel between a POP3 client with IP address 192.168.1.5 and a POP3 server with address 193.165.1.10. The tunnel starts at the POP3 client's machine on port 50000 and ends at the POP3 server machine. Which of the following <address, port> pairs should the POP3 client connect to in order to use the SSH tunnel. **[d]**

a. 193.165.1.10 port 110
b. 193.165.1.10 port 22
c. 127.0.0.1 port 110
d. 127.0.0.1 port 50000
e. 127.0.0.1 port 22
f. 193.165.1.10 port 50000

2. In a system that implements the Bell LaPadula security model, Bob is a manager and has security level 1, and Alice is an employee and has security level 2. Security level 1 is higher than security level 2. Which of the following accesses is **NOT** allowed. **[d]**

a. Bob reads a file that Alice created
b. Bob writes to a file that he created
c. Bob reads a file that he created
d. Alice reads a file that Bob created
e. Alice writes to a file that she created
f. Alice reads a file that she created

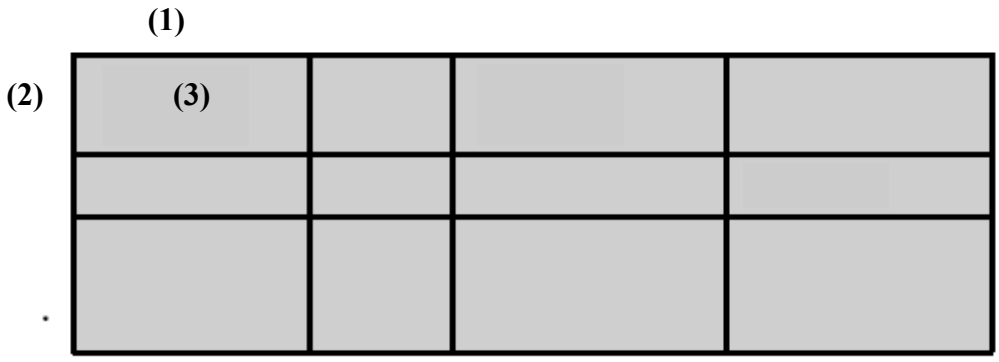
3. The following figure depicts a reference monitor blocking a Trojan Horse attack, whereby Alice has tricked Bob into running a Trojan Horse program that she wrote. The Trojan Horse reads from Bob's data file and writes into Alice's back-pocket file. Given that Alice has a lower security level than Bob's, which security policy is the reference monitor enforcing in the figure? **[c]**



a. no read up
b. authentication
c. no write down
d. integrity

e. no execute f. no read down

Questions 4-8 refer to the following figure, which depicts an access control matrix.



Access Matrix

For each question choose an answer from the following:

a. read and write b. file
c. capability ticket d. process
e. digital signature f. access control list

4. Label (1) may refer to: **b**
5. Label (2) may refer to: **d**
6. Label (3) may refer to: **a**
7. A column in the matrix is called: **f**
8. A row in the matrix is called: **c**

9. The IPSec protocol implements security at which network layer? **[c]**

a. physical b. data link
c. network d. transport
e. application f. session

10. The Secure Shell (SSH) protocol implements security at which network layer? **[e]**

a. physical b. data link
c. network d. transport
e. application f. session

11. In the IPSec protocol, which of the following security services is **NOT** provided by the Authentication Header (AH)? **[a]**

a. confidentiality b. authentication
c. anti-replay d. integrity

12. An IP packet is secured using IPSec. In which of the following IPSec modes does the original IP header of the packet get encrypted? **[d]**

a. AH in tunnel mode
b. ESP in transport mode
c. AH in transport mode
d. ESP in tunnel mode
e. both (a) and (d)
f. both (b) and (d)

13. Which of the following IPSec header fields help an IPSec gateway to identify the encryption algorithm used for encrypting the IPSec packets that it receives? **[f]**

a. IP destination address
b. Security parameter index
c. IP source address
d. Security protocol identifier
e. (a) and (c)
f. (a) and (b) and (d)
g. (a) and (d)

14. A TCP packet is sent over an IPSec Virtual Private Network (VPN). In which of the following IPSec operation modes does the TCP header of the packet get encrypted? **[f]**

a. AH in tunnel mode
b. ESP in transport mode
c. AH in transport mode
d. ESP in tunnel mode
e. both (a) and (d)
f. both (b) and (d)

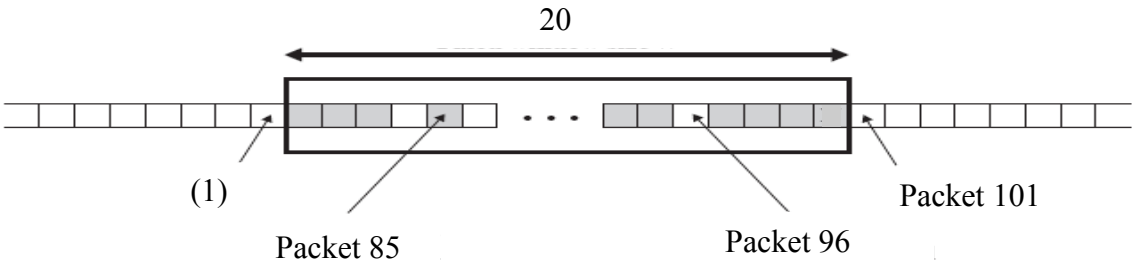
15. IPSec's Authentication Header in transport mode is used to secure an IP packet. Which of the following packet fields is **NOT** used to create the Message Authentication Code (MAC)? **[e]**

a. IP source address
b. IP destination address
c. TCP port number
d. header length
e. Time to Live
f. version
g. none of the above

16. IPSec's Authentication Header in tunnel mode is used to secure a packet. Which of the following fields of the packet is **NOT** included in the Message Authentication Code (MAC)? **[g]**

a. IP source address
b. IP destination address
c. TCP port number
d. header length
e. Time to Live
f. version
g. none of the above

Questions 17-23 refer to the following figure, which depicts a snapshot of the anti-replay mechanism in IPSec. The last valid packet received is packet number 100.



17. Label (1) refers to packet number: **[c]**

a. 20 b. 100
c. 80 d. 90

18. The figure indicates that packet 85 has been **[c]**

a. received invalid b. not received
c. received valid d. either (a) or (b)

19. The figure indicates that packet 96 has been **[d]**

a. received invalid b. not received
c. received valid d. either (a) or (b)

20. Which of the following packet reception events indicate a possible replay attack given the above figure: **[c]**

a. packet 96 b. packet 84
c. packets 102, 103, 104, 105, 84 d. packets102, 103, 104, 105, 96

21. The sliding window size is **[b]**

a. 100 b. 20
c. 80 d. 85

22. The packet numbers in the figure represent **[d]**

a. source address b. TCP sequence number
c. destination address d. IPSec sequence number

23. Which of the following packets causes the sliding window to be advanced? **[b]**

a. 100 b. 102
c. 80 d. 20