**INFA 620 - NETWORK AND INTERNET SECURITY**

**Final Exam**

***Instructions***

**Part 1:  Multiple Choice Questions. *Unless specified otherwise all multiple choice questions have only one correct answer.* Each question is worth 5 points.**

**PROBLEM 1 - Wireless Network Security (20 points)**  
(5 pts each)

a) What is the protocol developed for the wireless network communications? Explain.  
  
A) Wireless Encryption Protocol (WEP)  
B) Wireless Application Protocol (WAP)   
C) Wired Equivalent Privacy (WEP)   
D) Wireless Session Protocol (WSP)

b) Consider 802.11 shared key authentication. Which of the following statements is false? Explain.  
  
A) If a device with the key is lost then the security for the entire WLAN is compromised.  
B) 802.1X requires shared key authentication.  
C) Real users and attackers with a shared WEP key have the same rights.  
D) Users cannot determine whether the access point is an imposter.

c) The term used for certified 802.11b products is \_\_\_\_\_\_\_\_\_\_\_ .   
  
A) WAP   
B) Wi-Fi   
C) WiMAX  
D) WPA

d) Which of the following is not a reason why WEP may be considered vulnerable? Explain. (Select all that apply.)  
  
A) Shared WEP keys among all clients  
B) 20-bit initialization vector  
C) An RC4 engine not properly initialized  
D) 48-bit WEP key

**PROBLEM 2 - IPSec and VPN (20 points)**  
(5 pts each)

a) Select the term that refers to the data recipient's ability to ensure that the data was not altered in any fashion as the data was sent across the VPN:   
  
A) Encryption.  
B) Integrity.  
C) Authentication.  
D) Tunneling.

b) Tunneling is a technique in which the IP datagram is first \_\_\_\_\_\_\_ and then \_\_\_\_\_\_\_.  
  
A) Encapsulated in another datagram; encrypted.  
B) Encrypted; encapsulated in another datagram.  
C) Authenticated; encrypted.  
D) Encrypted; authenticated.

c) What is the relationship between a VPN and an extranet? Explain.  
  
A) Some extranets are VPNs; some VPNs are extranets.   
B) Some extranets are VPNs; all VPNs are extranets.   
C) VPNs and extranets are the same type of network.   
D) VPNs are unrelated to extranets.

d) Which one is the best approach to VPNs? Explain.  
  
A) VPN-specific gateway device.   
B) Router-based.   
C) Firewall-based.   
D) Software only.   
E) All of the above.

**PROBLEM 3 - Firewalls (20 points)**(5 pts each)

a) What governs the type of traffic that is and is not allowed through a firewall? Explain.  
  
A) TCP/IP headers.  
B) Gateway.  
C) Rule base.  
D) Access control list.  
E) Network protocol in use.

b) Firewalls can be implemented in different ways. Consider a dedicated firewall device. What is its major advantage when the target is throughput and security? Explain.  
  
A) The management console is easily installed.  
B) The device contains proprietary operating systems.  
C) The connection to the device is monitored by security personnel.  
D) A thorough packet inspection capability.  
E) The hackers know most router-based firewall code.

c) Choose the best answer from the following options about the description of a firewall:   
  
A) Firewalls statefully inspect reply packets to determine whether they match the expected state of a connection in the state table.  
B) Firewalls statically inspect packets in both directions and filter on layer 3and layer 4 information.  
C) A firewall is any device that blocks access to a protected network.   
D) A firewall is a system or a group of systems that enforce an access control policy between two networks.  
E) None of the above

d) For a stateful packet-inspection firewall, which information is stored in the connection flow table?   
  
A) TCP control header and trailer information associated with a particular session.  
B) Inside private IP address and the translated inside global IP address.   
C) Outbound and inbound access rules (ACL entries).   
D) Source and destination IP addresses, and port numbers and sequencing information associated with a particular session.   
E) TCP SYN packets and the associated return ACK packets.

**PROBLEM 4 - Web and Transport Layer Security (20 points)**  
(5 pts each)

a) Which of the following are not methods for minimizing a threat to a Web server? Indicate the two best answers from the following list, and explain your choice:  
  
A) Disable all non-Web services.  
B) Ensure telnet is running.  
C) Disable nonessential services.  
D) Enable logging.

b) SSL is used to  
  
A) Encrypt specific elements of data for application-specific purposes.  
B) Encrypt files located on a Web server.  
C) Encrypt data as it travels over a network.  
D) Encrypt digital certificates used to authenticate a Web site.  
E) Encrypt passwords for storage in a database.

c) What kind of attacks does SSL prevent? Select the best answer. Explain.  
  
A) SQL Injection.  
B) Sniffing.  
C) Variable Manipulation.  
D) Phishing Attacks.

d) \_\_\_\_\_\_\_\_\_ provides secure, remote logon and other secure client/server facilities.   
  
A) SLP  
B) HTTPS  
C) TLS   
D) SSH

[Delete everything above this prior to submission]

Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

First Last

INFA 620 FINAL

**Please put your answers in the following tables.**

|  |  |
| --- | --- |
| **Multiple Choice Questions** | **Answer** |
| 1a |  |
| 1b |  |
| 1c |  |
| 1d |  |
| 2a |  |
| 2b |  |
| 2c |  |
| 2d |  |
| 3a |  |
| 3b |  |
| 3c |  |
| 3d |  |
| 4a |  |
| 4b |  |
| 4c |  |
| 4d |  |

|  |  |
| --- | --- |
| **Multiple Choice Questions** | **Brief Explanations**  **If necessary** |
| 1a |  |
| 1b |  |
| 1c |  |
| 1d |  |
| 2a |  |
| 2b |  |
| 2c |  |
| 2d |  |
| 3a |  |
| 3b |  |
| 3c |  |
| 3d |  |
| 4a |  |
| 4b |  |
| 4c |  |
| 4d |  |

**Part 2: Short Answers. Please answer briefly and completely, and you must cite all sources of information. (20 points)**

1. Describe a method for protecting users against URL obfuscation attacks. **(10 points)**

2. A common management requirement is that “all external Web traffic must flow via the organization’s Web’s proxy.” However, that requirement is easier stated than implemented. Discuss the various problems and issues, possible solutions, and limitations with supporting this requirement. In particular, consider issues such as identifying exactly what constitutes “Web traffic” and how it may be monitored, given the large range of ports and various protocols used by Web browsers and servers. **(10 points)**

***--End—***