LAST NAME: _____

FIRST NAME: _____

UCID: _____

CPSC 526
Practice Midterm #2 Examination

True or False

Each of these statements is either *true* or *false*. Each answer is worth up to two points. A wrong answer or an empty answer is worth zero points. A correct answer is worth one point and a correct explanation is worth one point.

1. (2 points) Random sequence numbers in TCP make blind spoofing harder.
2. (2 points) TCP ISNs are designed to be hard to guess.
3. (2 points) DNSSec relies on encryption to secure delivery of DNS results.
4. (2 points) The SYN packet for a TCP connection always has a sequence number of 0.
5. (2 points) ARP poisoning is not a concern if the DHCP protocol runs correctly.

Multiple Choice

Each correct answer is worth two points. Each unanswered question or incorrectly answered question is worth zero points. You may include an explanation in your response. This explanation will not be marked, but if compelling may be used to give points to an otherwise wrong answer.

6. (2 points) What does DNSSec use to improve security for DNS results?
   (a) certificates
   (b) public key signatures
   (c) TLS encryption
   (d) TOFU for results
   (e) Kerberos tickets
7. (2 points) A DNS "NS" record is what?
   (a) a MAC address
   (b) a server name
   (c) an IP address
   (d) a DNS server
   (e) a domain name
8. (2 points) Suppose a TCP packet arrives to a recipient acknowledging data that has not yet been sent. What kind of a TCP packet is emitted by the recipient in response?
   (a) TCP SYN
   (b) TCP ACK
   (c) TCP RST
   (d) TCP FIN
   (e) such packets do not trigger a response
9. (2 points) Why is ARP vulnerable to ARP poisoning attacks?
   (a) because MAC addresses cannot be changed
   (b) because the MAC address to IP address is a fixed relation
   (c) because ARP query IDs are easily guessable
   (d) because ARP attacks can come from anywhere on the Internet
   (e) because ARP is a broadcast protocol

10. (2 points) Which network layer is used to communicate TLS public key certificates?
    (a) application
    (b) transport
    (c) network
    (d) link
    (e) physical

11. (2 points) Which network layer is used to communicate TCP resets?
    (a) application
    (b) transport
    (c) network
    (d) link
    (e) physical

12. (2 points) The DoS amplification attacks examples leveraged what kind of protocols?
    (a) TCP protocols
    (b) UDP protocols
    (c) ARP protocols
    (d) DHCP protocols
    (e) TLS protocols

Written Answers

Be sure to explain your answers in detail for this section and write in complete sentences.

13. (9 points) Suppose you wanted to determine whether a particular server uses SYN cookies. What is a means by which you, as a client who can connect to the server, may be able to determine that?

14. (10 points) Suppose a public DNS service receives far too many requests and cannot keep up. It decides to implement an anti-DoS feature to slow down the rate of client requests. If a client requests the IP for the same hostname multiple times in short succession is temporarily banned. Why will this not succeed in preventing DoS attacks?

15. (10 points) Suppose you wanted to test if a machine uses randomized ISNs. Detail (step-by-step) an experiment you can perform to assess this. State the data that you will look at and how the results will inform the answer to your question.