M6P1A1Solution CSS 211/ CS 459 Spring 2020 Covers: Chapter 6, Part I, of textbook

DATE ASSIGNED: February 25, 2020 DATE DUE: March 2, 2020 POINTS: 40

[A, 13 points] Multiple Choice

[A1]The strongest and most commonly used countermeasure against interception is

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) encryption (b) protection

[A2] The smallest individually addressable unit of data transmitted is

called a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) record (b) packet

[A3] \_\_\_\_\_\_\_\_\_\_\_\_\_ direct traffic on a path that leads to a destination. (a)

(a) routers (b) relays

[A4] A \_\_\_\_\_\_\_\_-day exploit is one for which an exploitation occurs before the vulnerability

is publicly known. (a)

(a) zero (b) first

[A5] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_are people who infect machines and turn them into bots. (a)

(a) Botmasters (b) Hackers

[A6] In the context of networks, “eavesdropping” or “wiretapping” refers to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) Interception (b) modification (c) fabrication (d) interruption

[A7] In the context of networks, “integrity failure” refers to \_\_\_\_\_\_\_\_\_ or \_\_\_\_\_\_\_\_. [(b), (c) or (c),(b)]

(a) Interception (b) modification (c) fabrication (d) interruption

[A8] In the context of networks, “denial of service” refers to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (d)

(a) Interception (b) modification (c) fabrication (d) interruption

[A9] A \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ advertises a network accepting connections. (a)

(a) beacon signal (b) authentication frame

[A10] A NIC requests a connection by sending \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ . (b)

(a) a beacon signal (b) an authentication frame

[A11] A(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a string to identify a wireless access point. (b)

(a) MAC address (b) SSID

[A12] The appeal of war driving has \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) increased (b) decreased

[A13] It is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to connect with any wireless signal detected. (b)

(a) legal (b) illegal

[B , 27 points] For each of the following, state if it is TRUE or FALSE.

[B1] By itself, cable is more secure than fiber. (F)

[B2] OSI is a 5-layer model. (F)

[B3] A frame contains the MAC addresses of the source and destination. (T)

[B4] Security through obscurity is an effective counter-measure. (F)

[B5] Replay attacks can succeed on encrypted data without altering or breaking the encryption. (T)

[B6] Port scanning can cause harm by itself. (F)

[B7] Redundancy can counter hardware failures. (T)

[B8] Misusing routing cannot cause denial of service. (F)

[B9] Denial-of-service attacks usually try to flood a victim with excessive demand. (T)

[B10] Any server can respond to a DNS lookup. (T)

[B11] Incapacitating the Internet’s DNS system itself can lead to denial of service. (T)

[B12] Session hijacking involves altering the source address in the IP protocol header. (T)

[B13] In a distributed Denial of Service attack botnets are marshalled on the victim’s side. (F)

[B14] Vulnerable machines cannot be discovered by scanning. (F)

[B15] A MAC address is 32 bits long. (F)

[B16] It is a good idea to use a MAC address for authentication. (F)

[B17] WEP security is acceptable. (F)

[B18] WPA fixes many shortcomings of WEP. (T)

[B19] Adding security after the design is fixed rarely succeeds. (T)

[B20] A Denial of Service attack can take the form of a Ping of Death attack. (T)

[B21] a Denial-of-Service attack pits one adversary against one target. (T)

[B22] The four types of harm that can occur in network communications are:

interception, modification, fabrication, interruption. (T)

[B23] Replay attacks cannot be countered with sequence numbers. (F)

[B24] Failure in the “last-mile” does not isolate the host. (F)

[B25] Wireless communication can be as secure as wired. (F)

[B26] The 802.11 protocol suite leaves wireless communications vulnerable. (T)

[B27] An operating system must send the correct MAC address of a NIC as the MAC address of that NIC.

(F)