M6P2A1Solution CSS 211/ CS 459 Spring 2020 Covers: Chapter 6, Part II, of textbook

DATE ASSIGNED: March 3, 2020 DATE DUE: March 9, 2020 POINTS: 30

[A, 13 points] Multiple Choice

[A1] A VPN commonly uses \_\_\_\_\_\_\_\_\_\_\_\_\_\_ encryption. (a) link

(a) link (b)end-to-end

[A2] SSL uses \_\_\_\_\_\_\_\_\_\_\_\_\_\_ encryption. (b)end-to-end

(a) link (b)end-to-end

[A3] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ hides real internal host addresses in a network. (b) NAT

(a) IPsec (b)NAT

[A4] Most IDSs have \_\_\_\_\_\_\_\_\_\_ network interfaces. (a) two

(a) two (b)three

[A5] The strongest tool for preserving confidentiality and integrity is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (c)encryption

(a) Firewall (b) IDS (c) Encryption

[A6] Users prefer \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ firewall. (a) default permit

(a) default permit (b)default deny

[A7] Security experts prefer \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ firewall. (b)default deny

(a) default permit (b)default deny

[A8] In \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , an administrator may redirect traffic to a valid address, where the incoming traffic can be analyzed. (b)

(a) Quenching (b) Sinkholing

[A9] A \_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a signal sent by a router back to a router that is forwarding traffic; such a signal informs the forwarding router that the receiving router is overloaded and cannot keep up, therefore asking the forwarder to hold up on transmitting data. (a)

(a) Quench (b) Sinkhole

[A10] A \_\_\_\_\_\_\_\_\_\_\_\_\_\_ mode IDS prevents the attacker from knowing that an alarm has been raised.

(a)

(a) Stealth (b) Stateful

[A11] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ inspection firewalls judge according to information from multiple packets. (b)

(a) Stealth (b) Stateful

[A12] A VPN simulates the security of a dedicated, protected communication line on a

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

(a) shared (b) non-shared

[A13] A personal firewall can work \_\_\_\_\_\_\_\_\_\_\_\_\_ support from the operating system. (b)

(a) without (b) only with

[B, 17 points] For each of the following, state if it is TRUE or FALSE.

[B1] SSL encrypts addressing data. (F)

[B2] Onion routing defends against traffic analysis. (T)

[B3] The SSL protocol protects against a keylogging Trojan horse implanted in the user’s computer. (F)

[B4] A firewall is a reference monitor. (T)

[B5] An IPS is an IDS with a built-in response capability. (T)

[B6] In IPv4 a system at address A cannot send a packet that shows address B as its source. (F)

[B7] SIEM can create a security dashboard for SOC personnel. (T)

[B8] Search features provided by SIEMs give them almost IDS-like capabilities. (T)

[B9] Rate limiting can reduce the impact of an attack. (T)

[B10] Many studies show that most computer security incidents are caused by insiders or people

impersonating them. (T)

[B11] The two general modes of encryption are: signature-based, anomaly-based. (F)

[B12] Two general types of IDSs are: end-to-end , link. (F)

[B13] Blacklisting filters out all traffic from implicated addresses. (F)

[B14] The administrator can shun the target address, meaning that no traffic can go to that address.

(F)

[B15] SSH has a known vulnerability. (T)

[B16] IPSec cannot enforce both of confidentiality and authenticity. (F)

[B17] A guard is a sophisticated firewall. (T)