M5A1Solution CSS 211/ CS 459 Spring 2020 Covers: Chapter 5 of textbook

DATE ASSIGNED: February 18, 2020 DATE DUE: Feb. 24, 2020 POINTS: 39

[A, 13 points] Multiple Choice:

[A1] Anti-virus software must be in control \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ the operating system allows access to

objects that might contain viruses. (b)

(a) before (b) after

[A2] From a security standpoint, the most important aspect of operating systems is \_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) performance (b) access control to resources.

[A3] A single-user operating system is called a(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) executive (b) monitor

[A4] A multi-user operating system is called a(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) executive (b) monitor

[A5] An executive \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ a user. (a)

(a) supports (b) controls

[A6] A monitor \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ a user. (b)

(a) supports (b) controls

[A7] In a \_\_\_\_\_\_\_\_\_\_\_\_\_ user operating system, the only security issue is physical protection of the

computer, its programs and data. (a)

(a) single (b) multi

[A8] Protection for the memory area for a user becomes necessary in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) executives (b) monitors

[A9] Software that implements a virtual machine is called a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) sandbox (b) hypervisor (c) honeypot

[A10] An environment from which a process can have only limited , controlled impact on

outside resources is called a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (a)

(a) sandbox (b) hypervisor (c) honeypot

[A11] A system to lure an attacker into an environment that can be both controlled and monitored is

called a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (c)

(a) sandbox (b) hypervisor (c) honeypot

[A12] Every word in memory has extra bits stating the access rights to that word, in the memory

protection scheme \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (b)

(a) based on base and bound registers (b) based on a tagged architecture

[A13] The Kernel is the part of the operating system that performs the \_\_\_\_\_\_\_\_\_\_\_\_\_ level

functions. (b)

(a) highest (b) lowest

[B, 26 points] For each of the following, state if it is TRUE or FALSE.

[B1] Operating systems are not just for conventional computers; some form of an operating system

can be found on automobiles, smart phones, and other devices. (T)

[B2] At system boot time, early tasks do not constrain later tasks. (F)

[B3] Many operating system protection mechanisms have been supported by hardware. (T)

[B4] The smaller the level of object controlled, the easier it is to implement access control. (F)

[B5] System tools, such as antivirus code , “hook” into and become part of the operating system, and are

loaded with the operating system. (T)

[B6] The operating system must protect itself , in order to protect its users and resources. (T)

[B7] Operating systems implement the underlying tables supporting access control but not the

mechanisms that check for acceptable users. (F)

[B8] Analysis of audit logs can help prevent future security breaches. (T)

[B9] Virtualization can help make operating systems secure. (T)

[B10] Operating systems must support separation of objects, but not sharing of objects. (F)

[B11] Virtual memory techniques like segmentation and paging do not provide memory protection. (F)

[B12] The reference monitor is not part of the security kernel. (F)

[B13] The TCB part of a trusted operating system can be impaired by the non-TCB part. (F)

[B14] A trusted path prevents interference between a user and the security mechanism of an operating

system. (T)

[B15] ATM machines cannot be compromised by skimmers. (F)

[B16] Object reuse attacks can be prevented using object sanitization. (T)

[B17]Common criteria bundle features and assurance. (F)

[B18] The rootkit inserts itself in a layer between the hardware and the operating system; thus

the rootkit controls the operating system.(T)

[B19] Not all rootkits are malicious. (T)

[B20] A rootkit does not have privileges of root. (F)

[B21] Anti-virus software is an add-on to the operating system. (T)

[B22] Sometimes the operating system must allow access to more than the system needs. (T)

[B23]A programmer must be aware of page boundaries in a paging based operating system. (F)

[B24] A programmer is not conscious of segments in a segmentation based operating system. (F)

[B25] Simple, modular, loosely coupled designs present fewer opportunities to the attacker. (T)

[B26] Security seldom succeeds as an add-on. (T)