COMP3052 Computer Security

Session 07: Reference Monitor

Videoclip: Protection Mechanisms (CISSP Free by Skillset.com)

https://www.youtube.com/watch?v=d-vhxg_j1kM&t=324s

Videoclip: Linux Architecture 2/5: Kernel/Security/and more!

https://www.youtube.com/watch?v=85eINAowuMc

Videoclip: Segmented, Paged and Virtual Memory

https://www.youtube.com/watch?v=p9yZNLeOj4s

1. The properties of a reference monitor are captured by the acronym NEAT. Which is the following is not a property of a reference monitor?

(A) The reference validation mechanism must be Non-bypassable, so that an attacker cannot bypass the mechanism and violate the security policy.

(B) The reference validation mechanism must be Evaluable, i.e., amenable to analysis and tests, the completeness of which can be assured (verifiable). Without this property, the mechanism might be flawed in such a way that the security policy is not enforced.

(C) The reference validation mechanism must be Always invoked. Without this property, it is possible for the mechanism to not perform when intended, allowing an attacker to violate the security policy.

(D) The reference validation mechanism must be Tamper-proof. Without this property, an attacker can undermine the mechanism itself and hence violate the security policy.

(E) The reference validation mechanism must be Tolerable to all kind of security vulnerabilities and attacks.

Reference: Reference monitor. You know what it is, right?

https://community.infosecinstitute.com/discussion/112586/reference-monitor-you-know-what-it-is-right

1. The properties of a reference monitor are captured by the acronym NEAT. Which is the following is not a property of a reference monitor?

(A) The reference validation mechanism must be Non-bypassable, so that an attacker cannot bypass the mechanism and violate the security policy.

(B) The reference validation mechanism must be Evaluable, i.e., amenable to analysis and tests, the completeness of which can be assured (verifiable). Without this property, the mechanism might be flawed in such a way that the security policy is not enforced.

(C) The reference validation mechanism must be Always invoked. Without this property, it is possible for the mechanism to not perform when intended, allowing an attacker to violate the security policy.

(D) The reference validation mechanism must be Tamper-proof. Without this property, an attacker can undermine the mechanism itself and thence violate the security policy.

(E) The reference validation mechanism must be Tolerable to all kind of security vulnerabilities and attacks.

Reference: Reference monitor. You know what it is, right?

https://community.infosecinstitute.com/discussion/112586/reference-monitor-you-know-what-it-is-right

2. What are the essential characteristics of the reference monitor?

(A) It is versatile, accurate, and operates at a very high speed.

(B) It is tamper-proof, can always be invoked, and must be small enough to test.

(C) It is restricted, confidential, and top secret

Reference: Cyber Security MCQs

https://quizack.com/ecommerce-cyber-security/mcq/what-are-the-essential-characteristics-of-the-reference-monitor

2. What are the essential characteristics of the reference monitor?

(A) It is versatile, accurate, and operates at a very high speed.

(B) It is tamper-proof, can always be invoked, and must be small enough to test.

(C) It is restricted, confidential, and top secret

Reference: Cyber Security MCQs

https://quizack.com/ecommerce-cyber-security/mcq/what-are-the-essential-characteristics-of-the-reference-monitor

3. Which of the following statements pertaining to protection rings is false?

(A) They provide strict boundaries and definitions on what the processes that work within each ring can access.

(B) Programs operating in inner rings are usually referred to as existing in a privileged mode.

(C) They support the CIA triad requirements of multitasking operating systems.

(D) They provide users with a direct access to peripherals

Reference: VCEguide

https://vceguide.com/which-of-the-following-statements-pertaining-to-protection-rings-is-false-2/

3. Which of the following statements pertaining to protection rings is false?

(A) They provide strict boundaries and definitions on what the processes that work within each ring can access.

(B) Programs operating in inner rings are usually referred to as existing in a privileged mode.

(C) They support the CIA triad requirements of multitasking operating systems.

(D) They provide users with a direct access to peripherals

Reference: VCEguide

https://vceguide.com/which-of-the-following-statements-pertaining-to-protection-rings-is-false-2/

4. Which of the followings is malicious software that alters the regular functionality of an OS, takes full control on the targeted system, and acts as the system administrator on the victim's system?

(A) Virus
(B) Spyware
(C) Trojan horse
(D) Rootkit

Reference: Testbook

https://testbook.com/question-answer/_____-is-malicious-software-that-alters-the-regul--62b1a7ccaaad4a4ea8350814

4. Which of the followings is malicious software that alters the regular functionality of an OS, takes full control on the targeted system, and acts as the system administrator on the victim's system?

(A) Virus
(B) Spyware
(C) Trojan horse
(D) Rootkit

Reference: Testbook

https://testbook.com/question-answer/_____-is-malicious-software-that-alters-the-regul--62b1a7ccaaad4a4ea8350814

5. Which of the following statements SIGSEGV or SIGBUS is incorrect?

(A) SIGSEGV indicates an invalid access attempt to a valid physical address.

(B) SIGBUS indicates an access attempt to an invalid physical address.

(C) Stack overflow is a cause of SIGSEGV.

(D) An attempt to access a read-only location will cause a SIGBUS.

Reference: What Is Signal 11 SIGSEGV Error?

https://phoenixnap.com/kb/sigsegv#:~:text=The%20main%20difference%20between%20the,indicates%20an%20invalid%20physical%20address.

5. Which of the following statements SIGSEGV or SIGBUS is incorrect?

(A) SIGSEGV indicates an invalid access attempt to a valid physical address.

(B) SIGBUS indicates an access attempt to an invalid physical address.

(C) Stack overflow is a cause of SIGSEGV.

(D) An attempt to access a read-only location will cause a SIGBUS.

Reference: What Is Signal 11 SIGSEGV Error?

https://phoenixnap.com/kb/sigsegv#:~:text=The%20main%20difference%20between%20the,indicates%20an%20invalid%20physical%20address.