Exam Questions

Willard Rafnsson

August 8, 2022
IT University of Copenhagen

1. What are the three kinds of harm? (see CIA)
2. An attacker injects code into a process, making it run their shell command. With what privileges does the shell command run? What could it do to the system?
3. How do you prevent code injection attacks? (L2)
4. In *Catch Me If You Can*, Frank Abagnale uses weapons of influence to obtain a Pan-Am uniform. Which weapons of influence did he use? Justify your answer.
5. We don't know how to prevent all attacks. Instead, what do we do? (L3 end)
6. What are the three basic mechanisms for implementing security? (Gold Standard)
7. Why is logging important? What events do you log? What goes into a log entry?
8. What security principle does multi-factor authentication apply? Explain how.
9. What security principle must a reference monitor apply? Explain how.
10. Why is unauthenticated encryption bad?
11. Why is $h(x) = 16x + 15$ a bad cryptographic hash function?
12. How & why does TLS use both symmetric- and public-key cryptography?
13. Why does DAC fail, and MAC succeed, at thwarting the Trojan Horse attack?
14. Under what assumption is it secure to authenticate future transactions of a user with only the token (session cookie, OAuth access token) they obtained by logging in?
15. What kind of security issues in OAuth does Mutual TLS address?
16. How is MAC typically implemented in modern microservice architectures?
17. An IFC enforcement tracks *pc* to detect a certain kind of information flow. Name the flow, and explain what it is.
18. How does program analysis relocate a trust assumption? (B, W)
19. How does program transformation relocate a trust assumption? (B, W)
20. What can you, as a developer, do to help your team write secure software?