Auto-Evaluation and Review Questions
(OS Level Security)

1. What is the aim of system security planning?
2. What are the pros and cons of automated patching?
3. What means security hardening and why is it important?
4. What type of access control model do Unix and Linux systems implement?
5. What permissions may be specified, and for which subjects?
6. What commands are used to manipulate extended file attributes access lists in Unix and Linux systems?
7. What effect do set user and set group permissions have when executing files on Unix and Linux systems?
8. What is the main host firewall program used on Linux systems?
9. Why is it important to rotate log files?
10. How is a chroot jail used to improve application security?
11. Where are two places user and group information may be stored on Windows systems?
12. What are the major differences between the implementations of the discretionary access control models on Unix and Linux systems and those on Windows systems?
13. What are mandatory integrity controls used for in Windows systems?
14. What virtualization alternatives you know and what advantages you car ague for each virtualization technique ?
15. What are the main security concerns with virtualized systems (namely taking into consideration the virtualization techniques you described before in question 14)?

- - -

16. Set user (setuid) and set group (setgid) programs and scripts are a powerful mechanism provided by Unix to support "controlled invocation" to manage access to sensitive resources. However, precisely because of this it is a potential security hole, and bugs in such programs have led to many compromises on Unix systems. Detail a command you could use to locate all set user or group scripts and programs on a Unix system, and how you might use this information.
17. Suppose you operate an Apache-based Linux Web server that hosts your company's e-commerce site. Suppose further that there is a worm called "WorminatorX," which exploits a (fictional) buffer overflow bug in the Apache Web server package that can result in a remote root compromise. Construct a simple threat model that describes the risk this represents: attacker(s), attack-vector, vulnerability, assets, likelihood of occurrence, likely impact, and plausible mitigations.
18. Why is logging important? What are its limitations as a security control? What are pros and cons of

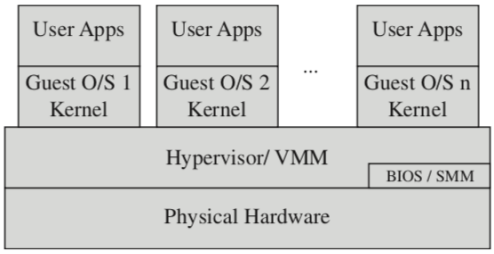
remote logging?

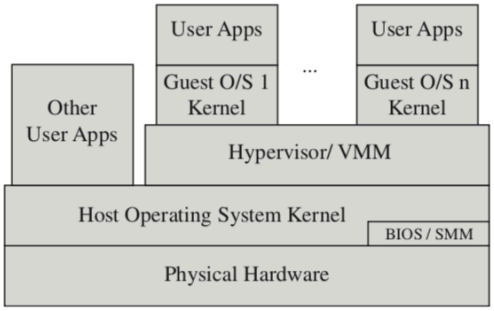
19. Make a proposal to design and implement a file-system integrity checking tool, describing how you could design and implement such a tool and how you propose that the tool would be used?

20. It is recommended that when using BitLocker on a laptop, the laptop should not use standby mode, rather it should use hibernate mode. Agree or not ? Why?

- - -

21. The following picture represents a virtualization architectural model and alternatives, representing virtualization options at different architectural levels. From the picture, try to sketch another picture, considering the architectural level of virtualization when you are using *docker* and dockerized applications or services.





22. Try to identify in the pictures related to question 21, the level of approach for the isolation support provided by a trust computing base materialized by a trusted-execution environment such as ARM TrustZone and Intel SGX technology