Безпека операційних систем і комп'ютерних мереж (Захист в інформаційно-коммунікаційних системах 2)

Питання до іспиту

1. Модель загроз для операційної системи
2. Типова архітектура комплексу засобів захисту операційних систем
3. Порівняльна характеристика підходів до побудови захищених систем
4. Критерії оцінювання захищених комп'ютерних систем Міністерства оборони США (TCSEC)
5. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ)
6. Стандарт ISO 15408: основні документи, структура профілю захисту і завдання з безпеки
7. Стандарт ISO 15408: структура стандарту, основні документи, структура вимог
8. Компоненти КЗЗ ОС Windows. Взаємодія компонентів і БД системи безпеки
9. Підсистема розмежування доступу ОС Windows. Суб'єкти і об'єкти доступу
10. Суб'єкти і об'єкти доступу ОС Windows. Реалізація дискреційного керування доступом
11. Алгоритми з'ясування прав доступу в ОС Windows
12. Реалізація підсистеми ідентифікації й автентифікації в ОС Windows
13. Архітектура і модель безпеки системи UNIX. Основні недоліки традиційної моделі безпеки UNIX
14. Підсистема ідентифікації та автентифікації UNIX. Підсистема розмежування доступу
15. PAM-автентифікація в Linux
16. Реалізація мандатного керування доступом і адміністрування безпеки у середовищі Trusted Solaris
17. Security Enhanced Linux: політики, контексти безпеки, операції
18. Процесори Intel i386: структури даних, що пов'язані з розмежуванням доступу до оперативної пам'яті
19. Процесори Intel i386: реалізація кілець захисту; привілейовані і чутливі команди
20. Процесори Intel i386: керування доступом до сегментів пам'яті під час звернень до нового сегмента та звернень за адресою у поточному сегменті
21. Процесори Intel i386: керування викликом процедур і задач
22. Загрози безпеці інформації у комп'ютерних мережах, віддалені атаки
23. ITU-T, рекомендації X.800. Основні сервіси і механізми безпеки в мережах

24. Проблеми протоколу IP і його реалізацій з точки зору безпеки інформації. Основні атаки на IP
25. Проблеми протоколу TCP і його реалізацій з точки зору безпеки інформації. Основні атаки на TCP
26. Безпека DNS. Можливі атаки
27. Протокол ICMP. Можливі атаки. Рекомендації із застосування
28. Проблеми протоколів Telnet і FTP. Уразливості. Методи захисту.
29. Безпека системи електронної пошти.
30. Безпека служби WWW: вразливості клієнтського ПЗ. Підвищення ступеня захищеності клієнтського ПЗ.
31. Безпека служби WWW: вразливості серверного ПЗ. Приклади атак.
32. Безпека CGI-застосунків: ін’єкції, методи захисту.
33. Міжмережні екрани. Класифікація, можливості й обмеження
34. Віртуальні приватні мережі (VPN). Сервіси віртуальних приватних мереж. Типи віртуальних приватних мереж
35. VPN віддаленого доступу. Протоколи PPTP і L2TP
36. VPN мережного рівня. IPsec (протоколи, режими, утворення захищених асоціацій)
37. VPN сеансового рівня: функції посередництва, протоколи
38. Засоби виявлення атак і протидії атакам