1. Современные угрозы сетевой безопасности
2. Векторы сетевых атак
3. Сети комплекса зданий
4. Сети небольших и домашних офисов
5. Сети центра обработки данных
6. Облачные и виртуальные сети
7. Термин «хакер»
8. Категории инструментов проведения атак
9. Типы вредоносного ПО
10. Термин «троянский конь»
11. Классификация троянских коней
12. Черви
13. Программы-вымогатели.
14. Шпионское ПО
15. Атаки для получения доступа
16. Разведывательные атаки
17. Типы сетевых атак
18. Фишинг
19. Руткиты
20. Типы атак для получения доступа
21. Социальная инженерия
22. Атаки «отказ в обслуживании»
23. DDoS-атаки
24. Конфиденциальность, целостность, доступность
25. Политика безопасности
26. Нейтрализация вредоносного ПО
27. Нейтрализация червей
28. Нейтрализация разведывательных атак
29. Нейтрализация атак для получения доступа
30. Нейтрализация DoS-атак
31. Защита сетевой инфраструктуры
32. Подходы к защите граничных маршрутизаторов
33. Три области защиты маршрутизатора
34. Безопасный локальный и удаленный доступ
35. Надежные пароли
36. Использование системного журнала
37. Протокол SNMP
38. Уязвимости SNMP
39. Спуфинг протокола маршрутизации
40. Режимы аутентификации
41. Авторизация
42. Методы аутентификации
43. Сравнение локальной и серверной аутентификации ААА
44. Аутентификация TACACS+
45. Аутентификация RADIUS
46. Использование аутентификации 802.1X на основе портов
47. Нумерованные и именованные списки ACL
48. Применение списка ACL
49. Защита от спуфинга с помощью списков ACL
50. Противодействие злоумышленному использованию протокола ICMP
51. Преимущества и ограничения межсетевых экранов
52. Преимущества и ограничения межсетевых экранов с фильтрацией пакетов
53. Межсетевые экраны с сохранением состояния
54. Принцип работы классического межсетевого экрана
55. Демилитаризованные зоны
56. Зональные межсетевые экраны (ZPF)
57. Преимущества зональных межсетевых экранов (ZPF)
58. Атаки нулевого дня
59. Технологии – IDS и IPS
60. Хостовая реализация IPS
61. Сетевые реализации IPS
62. Аппаратное и программное шифрование локальных данны
63. Зеркалирование портов
64. Категории атак на коммутаторы
65. Частные сети VLAN
66. Нейтрализация атак ARP
67. Создание и взламывание секретных кодов
68. Криптоанализ
69. Криптографическая хеш-функция
70. MD5 или SHA
71. Типы криптографических ключей
72. Два класса алгоритмов шифрования
73. Симметричное блочное и поточное шифрование
74. Алгоритм Диффи-Хеллмана
75. Алгоритмы с асимметричными ключами
76. Использование цифровых подписей
77. Цифровые сертификаты
78. Структура PKI
79. Сети IPsec VPN 3-го уровня
80. Два типа сетей VPN
81. Технологии IPsec
82. Сравнение IPsec и SSL
83. Протокол Authentication Header (AH)
84. Протокол Encapsulation Security Protocol (ESP)
85. Транспортный и туннельный режимы VPN
86. Протокол IKE
87. Топология сети IPsec VPN между двумя пунктами
88. Типы сетевых тестов
89. Инструменты тестирования сети
90. Иерархия политики безопасности