Вопросы к экзамену по учебной дисциплине «Фильтрация трафика в корпоративных сетях» (3 семестр)

1. Определение сетевого трафика и его классификация.
2. Методы анализа сетевого трафика.
3. Поверхностный анализ пакетов. Технологии реализующие SPI. Port-security. DHCP snooping.
4. Учёт состояния потока при анализе сетевого трафика.
5. Общая схема инфраструктурных алгоритмов анализа сетевого трафика. Система DPI.
6. Архитектура инструмента анализа трафика Wireshark.
7. Агрегирование пакетов в потоки и их анализ.
8. Сравнительная характеристика различных инструментов анализа трафика.
9. Определение фильтрации и проблемы, которые она может решить.
10. Функции фильтрации и типы.
11. Фильтрация на основе использования прокси-сервера.
12. Особенности фильтрации на основе технологии межсетевого экрана.
13. Основные компоненты систем фильтрации и их назначение.
14. Назначение и функции межсетевых экранов.
15. Отличия соединений SSH, Telnet и Serial.
16. Способы включения межсетевого экрана в сеть.
17. Типы портов межсетевого экрана и их функции.
18. Режим работы межсетевого экрана NAT/Route.
19. Режим работы межсетевого экрана Transparent.
20. Отличия и особенности настройки режимов работы межсетевого экрана.
21. Назначение виртуальных локальных сетей, достоинства и недостатки. Формат Ethernet-кадра в сетях VLAN и процесс его передачи.
22. Механизм реализации атаки VLAN-hopping. Уязвимости DTP.
23. Механизм реализации атаки MAC-spoofing. Методы защиты от атаки MAC-spoofing.
24. Принципы настройки виртуальных локальных сетей. Назначение протокола VTP, его преимущества, недостатки. Роли коммутаторов по протоколу VTP.
25. Назначение и принцип работы ACL.
26. Типы ACL и их отличия. Отличительные особенности настройки стандартных и расширенных списков контроля доступа.
27. Динамические и рефлексивные списки доступа.
28. Назначения DLP-систем.
29. Системы предотвращения вторжения.

30. Определение и назначение демилитаризованной зоны.
31. Политики безопасности для сети с DMZ.
32. Способы организации сети с DMZ.
33. Особенности настройки DMZ на межсетевом экране.
34. Правила прохождения трафика в сети с демилитаризованной зоной.
35. Протоколы мониторинга событий. Назначение протокола NetFlow.
36. Системы предотвращения вторжения, назначение, цель использования.
37. Различия между DoS и DDoS атаками. Типы DoS и DDoS атак. Примеры реализации атаки Ping Flood. Последовательность действий при атаке Ping flood.
38. Назначение утилиты hping3. Примеры ее использования для реализации DoS атак.
39. Принципы построения защиты от DoS атак на межсетевом экране. Описания аномалий и их конфигураций.
40. Принципы реализации SYN атак, пример. Принцип реализации UDP Flood атаки, пример.
41. Назначение и основные функции устройств защиты электронной почты.
42. Особенности конфигурации профилей защиты на устройствах защиты электронной почты.