Содержание ТУ (ДВИК.40006-15 ТУ) на АПК "Аргус" версии 1.5

6.2.22 Наличие механизмов генерации и записи в журнал событий сообщений об аномальной длине IP-датаграммы
6.2.23 Наличие механизмов генерации и записи в журнал событий сообщений об аномальной длине IP-фрагмента
6.2.24 Наличие механизма сборки полезных данных TCP-сессии
6.2.25 Наличие механизмов генерации и записи в журнал событий сообщений об перекрывающихся сегментах TCP-сессии, содержащих различные данные перекрывающихся областей
6.2.26 Наличие механизмов генерации и записи в журнал событий сообщений об перекрывающихся сегментах TCP-сессии, содержащих одинаковые данные перекрывающихся областей
6.2.27 Наличие механизмов выявления скрытых ICMP-туннелей, позволяющих генерировать и записывать сообщения об ICMP-туннелях в журнале событий
6.2.28 Наличие механизмов выявления скрытых HTTP-туннелей, позволяющих генерировать и записывать сообщения о HTTP-туннелях в журнале событий
6.2.29 Наличие механизма выявления прикладного протокола «SMTP» на основании заданной статической таблицы известных SMTP-портов, позволяющего проводить детальный анализ полей протокола SMTP
6.2.30 Наличие механизма выявления прикладного протокола «SMTP» на основании динамического анализа данных, позволяющего проводить детальный анализ полей протокола SMTP
6.2.31 Наличие механизма выявления прикладного протокола «POP3» на основании заданной статической таблицы известного POP3-порта, позволяющего проводить детальный анализ полей протокола POP3
6.2.32 Наличие механизма выявления прикладного протокола «POP3» на основании динамического анализа данных, позволяющего проводить детальный анализ полей протокола POP3
6.2.33 Наличие механизма выявления прикладного протокола «HTTP» на основании заданной статической таблицы известных HTTP-портов, позволяющего проводить детальный анализ полей протокола HTTP
6.2.34 Наличие механизма выявления прикладного протокола «HTTP» на основании динамического анализа данных, позволяющего проводить детальный анализ полей протокола HTTP
6.2.35 Наличие механизма выявления прикладного протокола «DCE RPC» на основании заданной статической таблицы известных портов DCE RPC, позволяющего проводить детальный анализ полей протокола DCE RPC
6.2.36 Наличие механизма выявления прикладного протокола «SUN RPC» на основании заданной статической таблицы известных портов SUN RPC, позволяющего проводить детальный анализ полей протокола SUN RPC
6.2.37 Наличие механизма выявления прикладного протокола «DNS» на основании заданной статической таблицы известных портов DNS, позволяющего проводить детальный анализ полей протокола DNS
6.2.38 Наличие механизма обнаружения атаки типа «FTP bounce», позволяющего генерировать и записывать сообщения об атаке в журнал событий
6.2.39 Наличие механизма выявления некорректного использования команд SMTP (т.е. появление команд не соответствующих состоянию SMTP-сервера), позволяющего генерировать и записывать сообщения о некорректном использовании в журнал событий
6.2.40 Наличие механизма выявления хостов, рассылающих спам или вирусы по средствам электронной почты, позволяющего генерировать и записывать сообщения о факте рассылки в журнал событий
6.2.41 Наличие механизма анализа кодированного трафика HTTP средствами gzip и zlib(deflate), позволяющего проводить детальный анализ полей протокола HTTP
6.2.42 Наличие механизма генерации и записи в журнал событий сообщений о превышении заданной максимальной длины HTTP-заголовка
6.2.43 Наличие механизма генерации и записи в журнал событий сообщений о превышении заданной максимальной длины тела полезных данных HTTP-запроса
6.2.44 Наличие механизма генерации и записи в журнал событий сообщений о факте двойной кодировки URL

6.2.45 Наличие механизма генерации и записи в журнал событий сообщений об обнаружении HTTP-канала управления БОТ-сетью
6.2.46 Наличие механизма генерации и записи в журнал сообщений, содержащих информацию о неактивных пользователях IRC-каналов
6.2.47 Наличие механизма генерации и записи в журнал событий сообщений о подборе пароля к учетной записи почтового сервера и превышении заданного предела неправильных POP3-логинов за заданный интервал времени с одного или нескольких хостов в сети
6.2.48 Наличие механизма обнаружения некорректного использования протокола POP3 (т.е. обнаружение команд, не соответствующих состоянию POP3-соединения), позволяющего генерировать и записывать сообщения о некорректном использовании в журнал событий
6.2.49 Наличие механизма выявления нарушений в трафике с использованием корреляционного анализа обоих направлений трафика и ведения статистики нарушений по времени, с записью соответствующих сообщений в журнал событий
6.2.50 Наличие механизма фильтрации трафика по IP-адресу источника и получателя, передаваемого для дальнейшего сигнатурного анализа
6.2.51 Наличие механизма фильтрации трафика по типу протокола, передаваемого для дальнейшего сигнатурного анализа
6.2.52 Наличие механизма фильтрации трафика по типу объектов протокола: порту, хосту, сети, диапазону портов, передаваемого для дальнейшего сигнатурного анализа
6.2.53 Наличие механизма фильтрации трафика по значениям полей протоколов, передаваемого для дальнейшего сигнатурного анализа
6.2.54 Наличие механизма задания логических операций при фильтрации трафика, передаваемого для дальнейшего сигнатурного анализа
6.2.55 Наличие механизмов управления контекстом соединения TCP-сессии, позволяющих рассматривать любые последовательности TCP-пакетов корректной TCP-сессией
6.2.56 Требование по наличию средств обнаружения DOS-атак средствами сигнатурного анализатора, генерирующих и записывающих в журнал событий сообщения об обнаруженных DOS-атаках
6.2.57 Наличие средств табличного и графического представления отчетов по накопленной статистике атрибутов трафика
6.2.58 Требование по наличию средств табличного и графического представления отчетов по накопленной Netflow-статистике атрибутов трафика, позволяющих обнаруживать DOS/DDOS атаки
6.2.59 Наличие средств передачи сообщений СОА и Netflow-потоков внешним получателям
6.2.60 Наличие средств регистрации, вывода сообщения и фильтрации на консоль управления при обнаружении компьютерной атаки
6.2.61 Наличие средства оповещения о событии по электронной почте
6.2.62 Требование по маскированию СОА в составе контролируемой АИС
6.2.63 Наличие механизмов разграничения прав доступа для пользователей
6.2.64 Наличие уведомления на электронную почту о факте подбора пароля
6.2.65 Наличие средств проверки целостности файловой системы
6.2.66 Наличие средств проверки синтаксиса загружаемых политик (сигнатур) пользователя
6.2.67 Запрещение прямого доступа к файловой системе и процессам операционной системы
6.2.68 Наличие средств обновления политик (сигнатур) через USB-flash диск, FTP сервер и WEB-интерфейс
6.2.69 Наличие средств добавления политик (сигнатур) пользователя
6.2.70 Наличие средств включения/выключения набора политик для анализа
7. Транспортирование и хранение
7.1. Требования к транспортировке
7.2. Требования к хранению
8. Гарантии изготовителя
Приложение 1. Схема испытательного стенда
Лист регистрации изменений