

Список литературы

1. ТКП 45-4.02-273-2012. ПДЗ зданий и сооружений при пожаре. Системы вентиляции.
2. СНБ 4.02.01. Отопление, вентиляция и кондиционирование воздуха.
3. НПБ 23-2010. ПДЗ зданий и сооружений. Методы испытаний.

МЕТОДИКА НАСТРОЙКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СЕТИ

А.А. Горелик, Н.В. Журавский

В работе [1] для оценки защищенности узлов информационной сети предложено использовать программное средство «Сканер». В настоящей работе определен порядок настройки и эксплуатации указанного средства. Он включает в себя следующие этапы.

1. Вход в веб-интерфейс ПС «Сканер». Для этого необходимо открыть веб-обозреватель и перейти по адресу <https://<IP-адрес сервера ПС «Сканер»>/>. В результате будет открыто окно авторизации, в котором необходимо ввести имя пользователя и пароль.

2. В случае успешной авторизации – выбор ссылки «Задачи» в разделе «Сканирование» главного меню.

3. Запуск процесса сканирования. Для запуска стандартного сканирования следует выбрать «Мастер задач» и в открывшемся диалоговом окне указать IP-адрес или DNS-имя целевой системы (устройства). Для запуска расширенного сканирования в окне «Продвинутый мастер задач» необходимо выбрать дополнительные параметры сканирования, основными из которых являются следующие:

- «Конфигурация сканирования» – выбор предустановленной конфигурации сканирования;
- «Время запуска:» – время запуска задачи сканирования (немедленно или по расписанию);
- «Отправить отчет по электронной почте» – адрес электронной почты для отправки отчета.

4. Формирование отчета, содержащего результаты сканирования.

На основе данных, представленных в отчете, составляются рекомендации по совершенствованию механизмов защиты данных в исследованном объекте (информационной системе или информационной сети).

Список литературы

1. Горелик А.А., Бойправ О.В., Журавский Н.В. Методика анализа защищенности узлов вычислительной сети // Материалы XV Международной науч.-практ. конф. «Управление информационными ресурсами», Минск, 7 декабря 2018 г. С. 210–212.

ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК С ПОМОЩЬЮ ТЕХНОЛОГИИ HONEYPOT

В.И. Грицкевич, С.Н. Петров

В современном информатизированном мире для любой организации очень важно защитить свои активы от нападения злоумышленников. Чтобы приблизиться к обеспечению наиболее полной информационной безопасности, нужно быть на шаг впереди злоумышленников, таким образом, необходимо отражать атаки до наступления негативных последствий от их выполнения. Одним из таких инструментов для мониторинга поведения злоумышленников является технология Honeyrot (далее – ханипот).

В ходе анализа существующих ханипотов был сделан вывод, что хорошим вариантом построения данной технологии является комбинирование автоматического подхода к решению задачи обнаружения атак и человеческих возможностей принятия решения. Архитектура такой системы может состоять из четырех различных компонентов, а именно: внешний брандмауэр, ханипот (виртуальная машина), база знаний и специальная группа SOC (Security operations center, центр реагирования на инциденты в сфере информационной безопасности) для ручного анализа журналов событий. В ней присутствуют различные модули для определения наиболее точных результатов, которые помогут администратору принимать решения на основе