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 Honeypot (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

автоматически генерируемых журналов событий. В рассматриваемом подходе задачей группы центра оперативного реагирования на инциденты в сфере информационной безопасности является ручной анализ данных из различных источников и принятие решения для какого-либо действия в зависимости от уровня критичности.

Ханипоты не могут полностью заменить такие средства защиты информации, как средства обнаружения вторжений или межсетевые экраны. Однако ханипоты являются прекрасным средством для изучения инструментария и методологии злоумышленников и улучшения систем защиты информации с помощью полученной информации. Помимо этого, благодаря возможности использования человеческих способностей для принятия решении о критичности события, ханипоты могут стать прекрасным дополнением функционирования центра оперативного реагирования на инциденты в сфере информационной безопасности (SOC).

Список литературы

1. Rahul Koul, Bakal J.W. Modern attack detection using intelligent honeypot // International research journal of engineering and technology. 2017. № 4. P. 2866–2869.

2. Назначение технологии Honeypot. [Электронный ресурс]. URL: https://www.securitylab.ru/analytics/275420.php?R=1 (дата обращения: 02.05.2019).

ОСОБЕННОСТИ ПОДГОТОВКИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В УСЛОВИЯХ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

М.В. Губич

Развитие информационного общества обусловило рост количества информации в электронном виде, подлежащей защите, и регистрируемых киберпреступлений, что в свою очередь повлекло необходимость подготовки квалифицированных кадров, обученных общим вопросам обеспечения информационной безопасности, и отдельной категории сотрудников, способных эффективно противодействовать преступлениям в сфере высоких технологий.

В связи с этим одной из основных целей профессиональной подготовки специалиста юридического профиля для правоохранительной сферы становится непрерывная компьютерная подготовка, в рамках которой должна быть сформирована готовность к использованию информационно-коммуникационных технологий (ИКТ), являющаяся базовой основой для развития компетенций в области информационной безопасности. К составляющим готовности к использованию ИКТ мы относим теоретические знания, технологические умения, навыки и профессиональные качества, личностные и мотивационные качества.

Соответственно, концепция формирования готовности к использованию ИКТ, на наш взгляд, должна быть основана на принципах обучения, способствующих овладению умениями решать профессиональные задачи и проблемы правоохранительной сферы на базовом (на уровне пользователя на основе выполнения установленных требований по информационной безопасности), углубленном (на уровне продвинутого пользователя, осуществляющего мероприятия по обеспечению информационной безопасности собственного рабочего места пользователя на основе выполнения требований технических и иных нормативных правовых актов) и специальном уровнях (умение решать служебные задачи на основе внедрения в служебную деятельность новых ИКТ, разработки собственных систем и средств обеспечения информационной безопасности рабочих мест пользователей ИКТ организации, а также противодействовать компьютерной преступности).

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ С ПОМОЩЬЮ ПОИСКОВОЙ СИСТЕМЫ SHODAN

Ш.Р. Давлатов

Shodan – это ведущая поисковая система по Интернету вещей, существующая уже более семи лет. В отличие от популярных поисковых движков (Google, Yandex, Bing и др.), которые ищут в сети информацию из обычных сайтов, система Shodan работает с теневыми каналами