

П. К. Лапко, А. В. Овсейчик

(ГГУ им. Ф. Скорины, Гомель)

УТИЛИТА ДЛЯ ПОИСКА И УСТРАНЕНИЯ

ИЗВЕСТНЫХ УЯЗВИМОСТЕЙ НА СЕРВЕРАХ

Так как Интернет всё больше внедряется в жизнь человека, он начинает распространяться на новые сферы жизнедеятельности. Работать с web-ресурсами начинают люди, часто не подготовленные к опасностям «всемирной паутины». Наряду с опытными администраторами, серверами начинают управлять специалисты без специальной подготовки в области защиты информации. В связи с этим появляются типичные ошибки в сетевых настройках, настройках безопасности, к которым добавляются известные уязвимости серверов. Такие ресурсы становятся целью и легкой добычей для злоумышленников.

Очевидно, что поиск и устранение уже известных ошибок и уязвимостей легко автоматизируем. Для этого можно использовать файлы настроек серверов, лог-файлы и информацию об установленном программном обеспечении. Полученную о сервере информацию можно использовать для сравнения с шаблонной настройкой. Необходимо учесть особенности различных операционных систем, устанавливаемых на серверах, а также программного обеспечения. Стоит помнить, что безопасность не статическое понятие, появляются всё новые и новые уязвимости. Чтобы обеспечить актуальное состояние защищённости необходимо постоянно обновлять информацию о существующих проблемах в безопасности и иметь постоянный доступ к этой информации.

Нами разрабатывается утилита, которая позволяет проверить некоторый сервер на наличие ошибок в сетевых настройках, настройках безопасности, выявить программные версии с известными уязвимостями.

Утилита использует базовый шаблон для поиска, но при необходимости может подключаться к серверу для обновления базы данных об уязвимостях. При обнаружении отклонений от эталонных настроек, утилита предлагает исправить ошибки. Автоматическое исправление невозможно, по сути, так как существует огромное множество различных конфигураций, необходимых на том или ином сервере, разнообразие которых невозможно предусмотреть.

Применение данной утилиты обеспечит базовый уровень защиты сервера, стабильную работу программ, установленных на нём, и избавит администратора от рутинного поиска неправильных настроек.