

УДК 50.41.00, 50.37.23

Д.А.Москвин (4 курс, каф. ИБКС), М.О.Калинин, к.т.н., доц.

АВТОМАТИЗИРОВАННЫЙ МОНИТОРИНГ НАСТРОЕК БЕЗОПАСНОСТИ MICROSOFT WINDOWS 2000/XP

Настройки безопасности информационных ресурсов влияют на защищенность компьютерной системы в целом. В процессе эксплуатации такой операционной системы (ОС) как Windows 2000/XP, пользователь вынужден оперировать огромным количеством защищаемых ресурсов (например, файлов, ключей реестра, принтеров) и их настройками. Для проведения качественного администрирования защищенных систем, построенных на базе указанной ОС, необходимо обладать всей полнотой информации об объектах системы, т.е. осуществлять мониторинг безопасности ОС.

В настоящее время известно два основных способа проведения мониторинга: «ручной» и автоматизированный. В первом случае необходимые данные получают посредством встроенных системных средств (например, с помощью редактора *regedit*, оснасток администрирования), что весьма неэффективно при большом количестве настроек, так как требует много времени и не дает гарантий полноты собранной информации. Во втором случае используют специальные утилиты, которые позволяют получать интересующие оператора настройки и отслеживать их изменения. Анализ рынка таких средств показывает, что большинство имеет существенные недостатки. Например, утилиты из состава *Resource Kit* (*subinacl* и др.) или такие популярные средства как *Security Explorer*, *WinObjEx* или *Process Explorer*, имеют ограничения по типам объектов и настроек, а также неудобный вывод результатов. Для решения указанных проблем разработано средство «Анализатор», предназначенное для проведения автоматизированного мониторинга и инвентаризации настроек безопасности всех именованных объектов защиты в среде Windows 2000/XP.

«Анализатор» собирает информацию о настройках безопасности следующих объектов: пользователи и группы, логические диски, каталоги и файлы, разделы и подразделы реестра, жесткие и символические ссылки, разделяемые ресурсы, службы, принтеры, СОМ-объекты, объекты режима ядра (процессы, потоки, задачи, маркеры безопасности, события, мьютексы, семафоры, таймеры, устройства, адаптеры, драйверы, контроллеры, порты, проекции файлов, профили, оконные станции, рабочие столы и др.). Для всех объектов есть возможность собрать данные о владельце и списке прав доступа, а также о специфических для каждого типа объекта атрибутах. Как результат? «Анализатор» генерирует файл-отчет, в котором содержится «снимок» подсистемы защиты в виде списка выявленных активных и пассивных участников безопасности со всеми настройками. Работа «Анализатора» основана на использовании низкоуровневого пользовательского интерфейса Windows 2000, функций ядра ОС, а также оригинальных алгоритмов обработки информации о структуре файловой системы NTFS и системного реестра.

Таким образом, в рамках работы разработано автоматизированное средство мониторинга, позволяющее оперативно собирать информацию о настройках безопасности ОС. «Анализатор» обладает рядом достоинств: наличие программного интерфейса для контроля всего процесса сбора информации; гибкость в задании множества собираемых настроек; сбор информации о всем множестве объектов защиты; достаточно высокая скорость сбора данных. Разработанное средство имеет широкую область применения. С его помощью администраторы могут регулярно проводить подробный анализ и отслеживать все изменения в защите ОС, а эксперты получают инструмент для получения «среза»

подсистемы безопасности. Разработанное средство также применимо в обучающих целях для исследования механизмов защиты Windows 2000/XP.