

## **СИСТЕМА МОНИТОРИНГА ОС WINDOWS SERVER. КЛИЕНТСКАЯ КОМПОНЕНТА**

А.М. КАДАН, А.А. ШАГУН

Задача создания системы мониторинга сетевого компьютерного оборудования достаточно актуальна, так как система мониторинга является неотъемлемой компонентой политики безопасности любой компании: позволяет решать задачи, связанные с планированием роста сети, поиском и устранением ошибок на серверном и сетевом оборудовании, анализом сетевого трафика.

В докладе представлена клиентская компонента системы мониторинга, разработанная для использования в рамках ОС Windows Server, которая реализует возможность постоянного наблюдения за состоянием узлов компьютерной сети: выполнять проверку доступности сетевых ресурсов, служб, следить за работой серверного и коммуникационного оборудования; в случае нарушения нормальной работы уведомлять администратора, используя различные средства оповещения.

При разработке данной системы были учтены недостатки известных решений. Главными преимуществами разработанной системы мониторинга ОС Windows Server является: простота настройки; легковесность решения; набор дополнительных функций, не имеющих аналогов. Эффективность разработанной системы продемонстрирована в сравнении с существующими решениями. Подтверждено, что разработанная система мониторинга в большинстве ситуаций потребляет меньше памяти и создаёт меньше нагрузки на процессор.

Оценивая функциональность, следует отметить, что в разработанной системе реализованы функции, которые отсутствуют в ее аналогах: мониторинг DHCP (система наблюдает за состоянием свободного пула адресов и ищет несанкционированные получения адреса); мониторинг DNS (анализ активных зон и уведомление пользователя об изменениях в них); мониторинг домена Active Directory (контроль над изменением групп пользователей, прав пользователей) и пр.

## **ГЕНЕРАЦИЯ СЛОВАРЕЙ НА ОСНОВЕ ИЕРАРХИЧЕСКИХ ПРАВИЛ В ЗАДАЧАХ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ**

А.М. КАДАН, Т.А. ПОШВА

Наиболее достоверную информацию, касающуюся компьютерных преступлений, позволяет получить компьютерно-техническая экспертиза. Данный вид исследования широко применяется при рассмотрении дел в гражданском и уголовном судопроизводстве и является одним из самых актуальных и востребованных.

Основной проблемой, с которой сталкивается эксперт при исследовании информации, является её недоступность. Зачастую важная информация защищена паролем и хранится в зашифрованном виде, и получить доступ к такой информации, без каких-либо знаний о ключе шифрования невозможно.

При наличии каких-либо данных о составителе пароля для взлома защищённой информации применяется метод атаки по словарю. В отличие от атаки полным перебором, проверяются не все возможные варианты, а лишь уже отобранные по специальным правилам до этого и загружаемые из списка слов, или словаря. Словарь генерируется из информации известной о составителе пароля или о самом пароле.

В докладе рассматривается разновидность простой словарной атаки и модели правил, которые позволяют пользователю задавать свои собственные варианты мутации элементов словаря. Рассмотрены системы иерархических разнородных правил, с помощью которых может быть описан механизм организации атаки. Выделены иерархические правила фильтрации — разнотипные иерархические правила, которые применяются к выходному