

## Заполнение матрицы данных о держателях карт, поиск PAN в системах

19.11.2009

*В статье рассказано о важных действиях первого шага на пути к соответствию PCI –определению систем, хранящих карточные данные и подготовке матрицы данных о держателях карт, а также показаны примеры технических средств, упрощающих данные действия.*

*Александр Поляков, руководитель направления аудита ИБ компании Digital Security, QSA*

Основной задачей стандарта, как вы уже наверняка все знаете, является обеспечение безопасности данных о держателях платёжных карт. И чуть ли не первым действием, после естественно решения о начале подготовки к системы к соответствию которое логично провести - это анализ того, где эти данные у нас в системе находятся и как передаются.

Другими словами это можно назвать составлением матрицы данных о держателях карт с описанием тех систем, где хранятся данные о держателях платёжных карт. Подробнее о матрице данных вы можете прочитать в статье Сергея Шустикова “Подготовка к аудиту – схема сети и матрица данных о держателях карт” (<http://pcidss.ru/articles/15.html>).

Кстати, аналогичные действия рекомендуются экспертами при составлении так называемой карты персональных данных, при подготовке к соответствию ФЗ-152 (<http://www.tsarev.biz/?p=790>). Данный подход более чем логичен, так как перед тем как разбираться, как защищать, не плохо бы понять, ГДЕ у нас находится то, что необходимо защищать, чтобы на следующем этапе по возможности уменьшить количество таких мест.

Составление матрицы данных в итоге значительно облегчит работу, как компании, так и консультантам или аудиторам, что в итоге значительно ускорит процесс первоначального анализа системы и сэкономит драгоценное время на решение задач связанных с подготовкой к сертификации и разработкой необходимых для соответствия решений.

Как оказалось, далеко не каждая компания может с уверенностью сказать, где конкретно в их системах хранятся данные о держателях карт (PAN), и даже если у компаний имеется хоть какая-то схема потоков данных, то на деле оказывается, что данные обнаруживаются в любых и даже самых неожиданных местах. Основные, но не единственные места, где можно обнаружить PAN - это trace, log, tlog, debug файлы СУБД, приложений и web-служб, а также файловые и почтовые сервера, рабочие станции операторов, POS –сервера и пр.

Составление матрицы данных - это первый этап выяснения мест нахождения PAN, но не последний, так как кроме известных мест всегда встречаются и неизвестные, поиск которых собственно позволяет

увидеть реальную картину. Для облегчения работ по обнаружению данных о держателях карт Советом PCI SSC были даны регулярные выражения для поиска PAN:

*Visa:* `^4[0-9]{12}(?:[0-9]{3})?$`

*MasterCard:* `^5[1-5][0-9]{14}$`

Эти регулярные выражения можно ввести в любую систему поиска, к примеру, встроенную в Total Commander и получить на выходе список файлов с PAN. После чего следует провести дополнительно проверку того, что найденная последовательность действительно является PAN по формуле mod 10 ([http://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC\\_%D0%9B%D1%83%D0%BD%D0%B0](http://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%9B%D1%83%D0%BD%D0%B0)).

На самом деле это только простейшие регулярные выражения, которые находят PAN, в котором нет разделителей между цифрами. В случае если в качестве разделителей используются пробел или тире, то необходимо применять более сложные регулярные выражения. К примеру, приведенное ниже выражение проверяет наличие номеров кредитных карт от Visa, MasterCard и Amex как в виде строки из цифр, так и с разделителями ([http://regexlib.com/REDetails.aspx?regex\\_id=340](http://regexlib.com/REDetails.aspx?regex_id=340)).

`^((4\d{3})|(5[1-5]\d{2}))(-?|\040?)(\d{4}(-?|\040?)){3}|^(3[4,7]\d{2})(-?|\040?)\d{6}(-?|\040?)\d{5}`

Для тех кто предпочитает делать данные проверки в автоматическом режиме в удобной оболочке со встроенной проверкой было разработано множество как коммерческих, так и бесплатных утилит для поиска PAN в системе.

Бесплатные утилиты:

- Spider (<http://www2.cit.cornell.edu/security/tools/>)
- ccsrch
- SENF
- FTimes
- Nessus
- Snort
- Open Source Forensic Tools

Коммерческие утилиты:

- Symantec Vontu
- RSA DLP Suite (Tablus)
- Vericept
- Orchestria

- Code Green Networks
- Reconnex
- Workshare
- Websense
- EnCase Forensic

Тема достаточно обширная и описать все существующие решения не представляется возможным, так что рассмотрим одну из бесплатных утилит, под названием Spider, которая выпущена сотрудниками университета Cornell, и позволяет искать в системах такие данные как номера кредитных карт (PAN), номера социального страхования и прочие данные.

Утилита имеет множество различных настроек позволяющих фильтровать поиск по последней дате изменения файлов, что актуально для проведения регулярных проверок, а также добавлять директории исключения и даже сканировать EFS разделы если к таким имеется доступ.

*Совет: при использовании данной утилиты изменить приоритет в диспетчере задач на “ниже среднего” Так как процедура поиска достаточно ресурсоёмка.*

На рисунке 1 изображен пример запуска утилиты Spider на директорию D:\WORK\, где мы можем наблюдать файл tlog.txt, в котором обнаружены PAN.

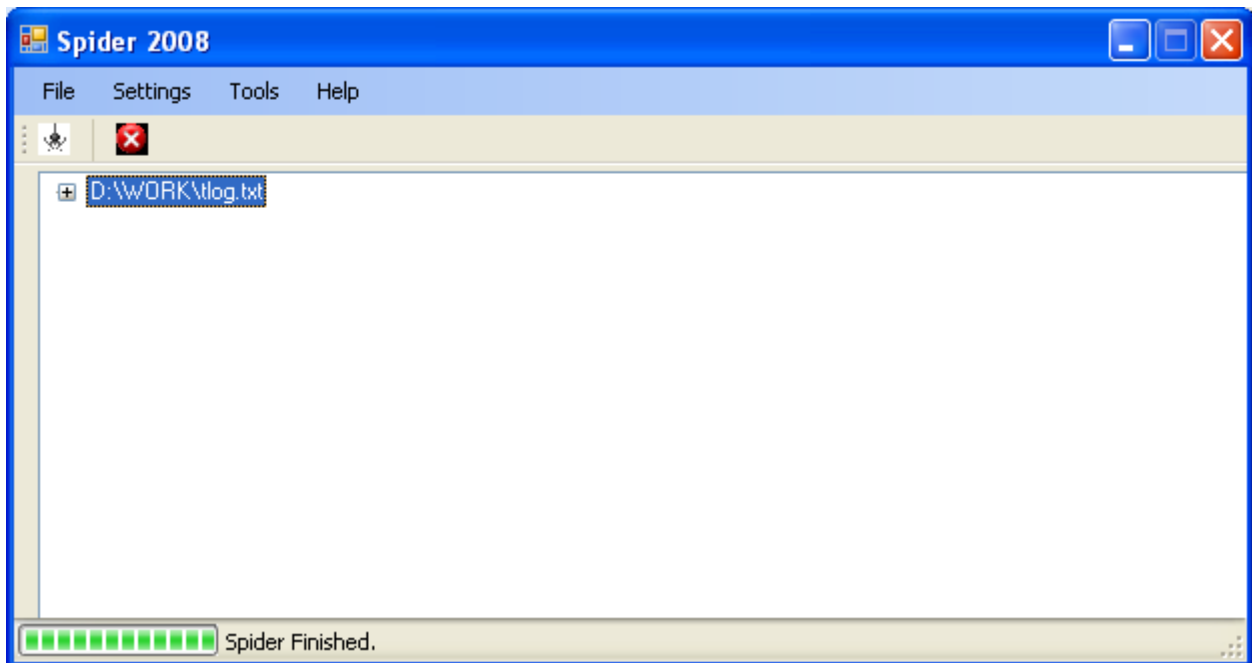


Рис. 1. Утилита Spider

После использования не забудьте удалить лог файлы созданные утилитой. Директория, где хранятся лог-файлы указана во вкладке Settings->Runtime->Administrative options.

Данная утилита рассмотрена как один из возможных способов поиска PAN и рассмотрена лишь в качестве примера. В статье были рассмотрены основные способы поиска PAN, которые можно использовать на серверах и рабочих станциях. В следующих статьях будут рассмотрены особенности поиска PAN в СУБД а также обнаружение передачи PAN по сети.

## Об авторе

Александр Поляков - руководитель направления аудита ИБ компании Digital Security. Специализируется на проведении аудитов защищенности, тестов на проникновение, анализе защищенности бизнес приложений и исследовательской деятельности в области информационной безопасности. Является известным экспертом по безопасности бизнес приложений таких производителей как Oracle и SAP, обнаружившим и опубликовавшим информацию о большом количестве уязвимостей в приложениях данных производителей. Один из основателей и руководитель исследовательского центра Digital Security Research Group [DSecRG], занимающегося поиском и анализом уязвимостей приложений и операционных систем. Автор ряда статей и исследований по информационной безопасности, автор книги «Oracle глазами аудитора: нападение и защита».

## О стандарте PCI DSS

Стандарт PCI DSS (Payment Card Industry Data Security Standard) предназначен для обеспечения безопасности обработки, хранения и передачи данных о держателях платежных карт в информационных системах компаний, работающих с международными платежными системами Visa, MasterCard и другими. Стандарт разработан сообществом PCI Security Standards Council, в которое входят мировые лидеры на рынке платежных карт, такие как American Express, Discover Financial Services, JCB, MasterCard Worldwide и Visa International.

Под действие требований стандарта попадают банки, процессинговые центры, поставщики ИТ-услуг, торгово-сервисные предприятия, и иные организации, обрабатывающие транзакции по международным платежным картам. К части этих компаний международные платежные системы предъявляют требование о прохождении обязательного ежегодного аудита компанией, обладающей статусом QSA.

Текущая версия стандарта 1.2 выпущена 1 октября 2008 года.