

Всех аудиторов «посодют»?!

Юридические аспекты консалтинга в области ИБ

Сергей Гордейчик

Positive Technologies



Обвинительное заключение 1

Утечки информации - Пентест как гусарская рулетка

Кафедра экспериментального права

10:30 am July 12th, 2009




 [infowatch](#)



Пентест как гусарская рулетка

Так называемые пентесты (тесты на проникновение) часто проводятся с использованием вредоносных программ. Тот факт, что обладатель информации и оператор ИС дал своё согласие на доступ, никак не влияет на квалификацию действий пентестера по ст.273 УК. Доступ – это одно, а программы – совсем другое.

-  **Так называемые пентесты (тесты на проникновение) часто проводятся с использованием вредоносных программ. Тот факт, что обладатель информации и оператор ИС дал своё согласие на доступ, никак не влияет на квалификацию действий пентестера по ст.273 УК. Доступ – это одно, а программы – совсем другое.**

<http://infowatch.livejournal.com/43369.html>



Обвинительное заключение 2


Николай Пятизбязцев



Согласно требованиям п. 11.3. стандарта PCI DSS компанией, попадающей под действие стандарта, должны проводиться тесты на проникновение. Данные тесты могут выполняться как собственными квалифицированными сотрудниками, так и сторонней организацией. В связи с тем, что данные тесты представляют собой моделирование действий злоумышленника по проникновению в информационную систему кредитной организации или процессингового центра, здесь могут возникнуть определенные сложности.

Как уточняет Антон Карпов, аналитик компании Digital Security , QSA-аудитора, «под тестом на проникновение понимается санкционированное проведение атак на сетевом уровне и на уровне приложений на все публично доступные сервисы компании из сети Интернет (т. н. внешний тест на проникновение) и внутренние ресурсы, входящие в область аудита PCI DSS (т.е. внутренний активный аудит защищенности)»¹. При этом особо указывается, что тест на проникновение «поможет детально выявить реальные уязвимости, присутствующие в сети компании и могущие стать причиной утечки данных держателей карт»². В случае, если такая атака окажется успешной, компания, осуществляющая тест на проникновение, может получить доступ к следующей охраняемой законом информации: коммерческой, банковской тайне, персональным данным. Так как тестирующая компания действует на основании договора, то есть с санкции банка или процессинга, то доступ к коммерческой тайне будет легитимным, а вот на доступ к банковской тайне или персональным данным необходимо получить разрешение клиента банка, чья

конфиденциальная информация может стать известна третьей стороне. В этой ситуации практически любой практикующий юрист заявит вам, что согласно букве российского законодательства без наличия такого разрешения компрометация банковской тайны или персональных данных не только может, но и должна повлечь за собой уголовную ответственность.

 **В этой ситуации практически любой практикующий юрист заявит вам, что согласно букве российского законодательства без наличия такого разрешения компрометация банковской тайны или персональных данных не только может, но и должна повлечь за собой уголовную ответственность.**

http://www.plusworld.ru/journal/page163_1242.php




Обвинительное заключение 3



Комментирует старший следователь отдела по делам об особо опасных преступлениях в сфере экономической деятельности Следственного комитета при МВД России, майор юстиции, кандидат юридических наук Андрей Доронин:

На мой взгляд, автором настоящей статьи справедливо ставится вопрос о защите института банковской тайны и персональных данных при проведении тестов на проникновение аудиторскими, как внутренними, так и внешними. Если, например, представить, что в результате проведения тестовой атаки компьютерная система, в которой в течение нескольких лет формировалась клиентская база банка (содержащая персональные данные, номера банковских карт и т. д.), была заблокирована или уничтожена, можно говорить об умышленно совершенном неправомерном доступе к компьютерной информации – ст. 272 УК Российской Федерации.

В действительности представляется недопустимым тестировать таким образом безопасность действующих баз данных, содержащих банковскую тайну. Как вариант, лучше проводить соответствующие тесты на специально сделанных моделях.

 **Если, например, представить, что в результате проведения тестовой атаки компьютерная система, <...>, была заблокирована или уничтожена, можно говорить об умышленно совершенном неправомерном доступе к компьютерной информации – ст. 272 УК Российской Федерации.**

http://www.plusworld.ru/journal/page163_1242.php



Вместо «хакеров»...



U.S. Department of Justice
United States Marshals Service

WANTED

BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, update warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NCK) V721460021)

NAME:MITNICK, KEVIN DAVID
AKS(S):MITNIE, KEVIN DAVID
 HERRILL, BRIAN ALLEN

DESCRIPTION:

Sex:MALE
Race:WHITE
Place of Birth:VAN NUYS, CALIFORNIA
Date(s) of Birth:08/06/63; 10/18/70
Height:5'11"
Weight:190
Eyes:BLUE
Hair:BROWN
Skintone:LIGHT
Scars, Marks, Tattoos:NONE KNOWN
Social Security Number (s):550-39-5495
NCIC Fingerprint Classification:DQ9M2OPK13D1PM19PH09




Всех пентестеров «посодют?»



U.S. Department of Justice
United States Marshals Service

WANTED

BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NCJ_ VT21460021)

NAME:MITHIE, KEVIN DAVID
AKS(S):MITHIE, KEVIN DAVID
 MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex:MALE
Race:WHITE
Place of Birth:VAN NUYS, CALIFORNIA
Date(s) of Birth:08/06/63; 10/18/70
Height:5'11"
Weight:190
Eyes:BLUE
Hair:BROWN
Skintone:LIGHT
Scars, Marks, Tattoo:NONE KNOWN
Social Security Number (s):550-39-5495
NCIC Fingerprint Classification:DQPKJOPK1JDIPM15PH09







Почему пентесты?

- ☰ **Заказчики (и исполнители) зачастую не понимают сути и методик Penetration Testing**
- ☰ **По конференциям ходят странные люди, рассуждающие о «пентестах, как эмуляции действий злоумышленника»**
- ☰ **PCI DSS делает Pentest **обязательным**, для процессингов**
- ☰ **Pentest с высокой вероятностью будет «успешен»**
 - Если «не взломали», то вы нашли плохого подрядчика.
 - Если «взломали», то вы плохо работаете.



Почему 273?

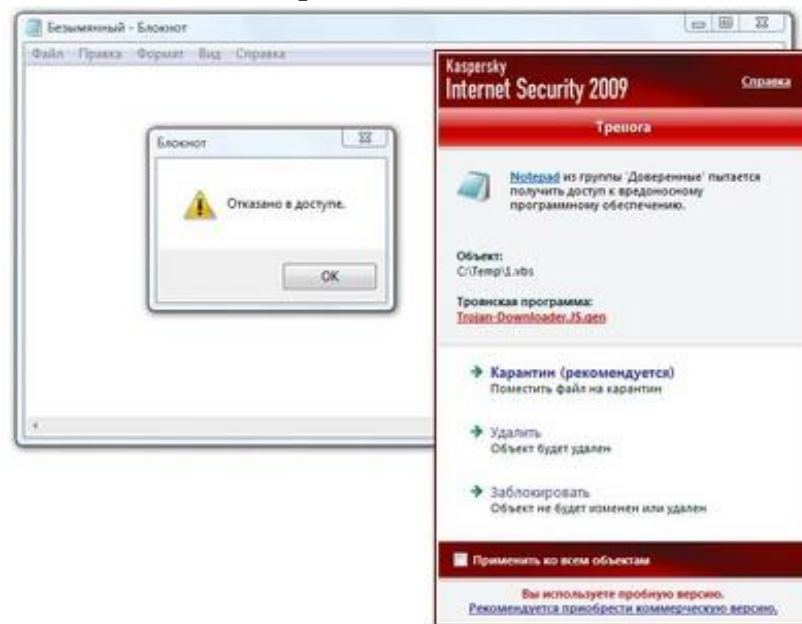
Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами

-  **формальный** состав преступления статьи 273 УК , т.е. наказуемы сами действия по созданию программ для ЭВМ
-  **отсутствие четких критериев** отделения вредоносного ПО от легальных программ



Что такое «вредоносное ПО»?

- ☰ Скопируем функцию (ресурсы [TechNet](#), [репозиторий скриптов](#)).
- ☰ Запишем функцию "GetHTTPCRL" в произвольный файл с расширением vbs.
- ☰ Удалим все комментарии из этого сценария и сохраним его.



<http://devteev.blogspot.com/2009/10/blog-post.html>



Что такое «вредоносное ПО»?

Периодически «вредоносным» оказывается самое разное ПО

AVG считает Adobe Flash вредоносным ПО

17 ноября, 2008



AVG
Anti-Virus System

Теги: AVG, антивирус, вредоносное ПО, Adobe F

Популярный антивирус AVG уже второй раз за не этот раз AVG по ошибке принял файлы Adobe Fla Ранее на неделе тот же продукт по ошибке приня злонамеренное программное обеспечение.

Чтобы загладить свою вину перед пользователями милости антивируса компания-производитель пре годовой лицензии на продукт.

Антивирус от Symantec заблокировал AOL

23 марта, 2006



Дополнение к базам определений вирусов от 15 марта, привело к семичасовой блокировке Пользователи, выходящие в Сеть через заблокированными.

Сигнатура обнаружения вторжения, поставленная провайдера как на источник атаки. В ре Security и Norton Personal Firewall вклю

<http://www.securitylab.ru/news/264376.php>

<http://www.securitylab.ru/news/363228.php>



Что делать?

- ☰ **Не использовать вредоносное ПО**
 - Не использовать общедоступные образцы вредоносного ПО.
 - Фиксировать согласие Заказчика на проведение конкретных атак на конкретные объекты для фиксации **санкционированного** доступа.
 - Взаимодействовать с антивирусными вендорами в рамках политики «Ответственного разглашения» для устранения обнаруженных недочетов в антивирусных программах.
 - Закладывать в разрабатываемое ПО ограничения, с целью предотвращения его несанкционированное использование.



В тему и offtopic



Сергей Гордейчик

Владелец студии консалтинга и



вторник, 1 сентября 2009 г.

Всех пентестиров посодют?

Компании "Инфовотч" видимо надоели обвинения в нарушении тайны переписки, и они решили перевести внимание подставив экспертов в области тестирования на проникновение. Инкриминируют им не много, ни мало - 273 статью УК - т. Понятно, что все это глупости, и настоящие пентестеры не вредоносное программное обеспечение, а используют инструменты управления, НО!

Между пентестерами и антивирусной индустрией действует некоторый конфликт.

☰ Но иногда, в ходе глубоких Red Team Pentest заказчика интересует, сумеет ли "продвинутый" злоумышленник обойти комплекс средств защиты, куда входят и антивирусы...

В этой ситуации пентестерам приходится искать недостатки в антивирусных программах и разрабатывать "утилиты удаленного управления", обходящие защиту.

☰ <http://sgordey.blogspot.com/2009/09/blog-post.html>



Ищем, закрываем... снова ищем...

PT-2009-05: Отказ в обслуживании в CA Internet Security Suite

Рейтинг опасности:	Средний (4.9) AV:L/AC:L/Au:N/C:N/I:N/A:C		
Статус:	Исправлено		
Вектор:	Локальный		
Производитель:	Computer Associates (CA)		
ПО:	CA Internet Security Suite Plus 2009 CA Internet Security Suite Plus 2008 CA Internet Security Suite 2007		
Идентификатор:	PT-2009-05	Дата уведомления:	04.02.2009
CVE ID:	CVE-2009-0682	Дата исправления:	18.08.2009



Уязвимость обнаружена:
Никита Тараканов, Positive Technologies Research Team

PT-2009-06 - F-Secure

Рейтинг опасности:	Средний (4.7) AV:L/AC:M/Au:N/C:N/I:N/A:C
Статус:	Исправление отсутствует
Вектор:	Локальный
Производитель:	F-Secure
Статус уведомления	04.02.2009 - Производитель уведомлен 11.02.2009 - Получен ответ 16.02.2009 - Отправлена детальная информация 16.02.2009 - Получен ответ

Дней с момента уведомления производителя: **287**



Уязвимость обнаружена:
Никита Тараканов, Positive Technologies Research Team



<http://www.securitylab.ru/lab/>



Доступ к банковской тайне

- ☰ **Потенциальная угроза нарушения положений п. 2 ст. 857 ГК РФ**
- ☰ **Ст. 26 Федерального закона «О банках и банковской деятельности» упоминает аудиторские организации в контексте Федерального закона «Об аудиторской деятельности».**
- ☰ **Статья 183 УК, **формальный** состав преступлений, предусмотренный ч.1 и ч. 2.**
- ☰ **Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну**



Только ли Pentest?

**ВСЕ РАБОТЫ, СВЯЗАННЫЕ С
ДОСТУПОМ К ДАННЫМ!**



МЫ НЕ ПОЛУЧАЕМ ДОСТУП К ДАННЫМ!

СТО БР ИББС 1.1 2009 - 7.2.10 – аудит процессов

- У вас все хорошо?

Pentest – анализ уязвимостей систем

- Мы взломали сервер 1.1.1.1, там простой пароль.
- Нет, мы не смотрели, что в этом Oracle.

PCI DSS, раздел 4 (шифрование данных)

- У вас все зашифровано? Ну и отлично.
- А покажите... Нет, лучше не надо.



Как «лечить»?

Предоставить это Заказчику

- Совместные работы.
- Выполнение «опасных» операций представителем заказчика.
- «Обезличивание» результатов.

Обходить опасные места

- Не работать с данными 😊

Переложить на клиента

- включать в договоры с клиентами



Крайний случай

Система
протоколирования



Представитель Заказчика



Ноутбук Заказчика



Исполнитель

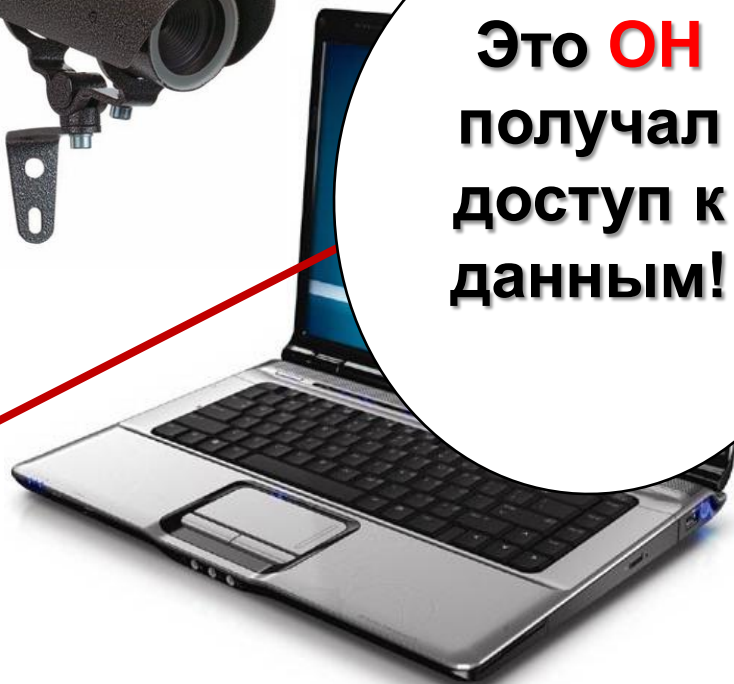


Крайний случай

Система
протоколирования



Представитель Заказчика



Это **ОН**
получал
доступ к
данным!

Ноутбук Заказчика



Исполнитель



Только ли аудиторы?

Техническая поддержка систем DLP

- У нас ХХХ не обрабатывает письма от YYY.
- Пришлите, пожалуйста перехваченную сессию.

Внедрение и поддержка систем АБС

- Даже подумать страшно!

Практически любые работы, связанные с ERP

- Он заходил в нашу 1С-Кадры!



Спасибо за внимание!

Сергей Гордейчик

gordey@ptsecurity.ru

<http://sgordey.blogspot.com>

<http://www.ptsecurity.ru>



POSITIVE TECHNOLOGIES