Тотальная Доминация

ЛОМАЕМ LOTUS DOMINO

Привет всем читателям. На этот раз я немного уйду в сторону от Oracle и расскажу про другое, не менее распространенное в корпоративной среде приложение — Lotus Domino. Domino — это такое огромное клиент-серверное приложение, совмещающее в себе и почтовую систему, и систему документооборота, и LDAP-хранилище, и еще множество всего, где может храниться полезная информация.

ОПИСАНИЕ

IBM Lotus Domino Server — сервер приложений системы Lotus, который предоставляет ряд сервисов и может использоваться для построения корпоративных систем электронного документооборота, которая имеет в своем составе большой набор модулей. Основные из них: почтовый сервер, HTTP-сервер и сервер баз данных. Так как в большинстве случаев во внешнюю сеть выставлен HTTP-сервер, то на его уязвимостях мы сосредоточим внимание. Проводить все грязные опыты будем на последней версии Lotus Domino 8.5.1 под Windows.

ГДЕ ОБИТАЮТ ЛОТУСЫ?

Собственно, для обнаружения в сети Web-сервера Lotus (Lotus Domino httpd) можно воспользоваться сетевым сканнером Nmap со следующими параметрами:

```
Nmap -sV 172.212.13.0.24 -p 80

Nmap scan report for 172.212.13.13
Host is up (0.017s latency).
Not shown: 65533 filtered ports
```

Так выглядит стартовая страница Lotus Domino

Так выглядит исходный код страницы с хэшем пароля

```
PORT     STATE SERVICE VERSION
80/tcp   open  http    Lotus Domino httpd
```

Судя по описанию, мы наткнулись на один из серверов Lotus, но для верности лучше проверить. Для того, чтобы убедиться, что это точно Lotus Domino httpd, можно обратиться по адресу: http://servername/homepage.nsf. Если мы увидим красивое окошко с номером версии, то, вероятнее всего, мы наткнулись на то, что искали.
На самом деле гораздо эффективнее будет воспользоваться методикой Google Hack и найти множество Lotus-серверов в интернете, используя простейший запрос inurl:homepage.nsf. В результате этого запроса нам откроются ссылки на тысячи потенциальных серверов Lotus. Сразу предупрежу тебя, чтоб ты даже не пытался тренироваться на этих серверах, так как у Лотуса очень навороченная и удобная система протоколирования всех запросов, и вычислить злоумышленника не составит труда.

ОСМОТР ПАЦИЕНТА

Итак, начнем анализ подопытного. Обычно при попытке обращения к корневой директории Lotus-сервера мы получаем окошко с запросом аутентификации, что сразу же отпугивает неопытных хакеров. Очень вероятно, что администратор установил запрос аутентификации только на обращение к корневой папке, а все остальные ресурсы остались открыты. Что же там могут быть за ресурсы, и чем они нам полезны?

ЗАГАДОЧНЫЙ .NSF

Если кратко, то Lotus хранит всю информацию в контейнерах собственного формата с расширением nsf. Данный контейнер представляет собой набор данных и формат их представления. Если говорить проще, то каждый nsf ресурс — это небольшой отдельный сайт со своей базой данных. Собственно, этих самых nsf-файлов может быть на сервере огромное количество, причем как стандартных, так и разработанных специально под нужды компании. Вот список наиболее популярных nsf-файлов, которые могут присутствовать:

```
/names.nsf
/admin4.nsf
/admin.nsf
/alog.nsf
/domlog.nsf
/catalog.nsf
/certlog.nsf
/dba4.nsf
/homepage.nsf
/log.nsf
```

Про остальные файлы ты можешь узнать, скачав, к примеру, утилиту dominohunter, к которой прилагается список стандартных nsf-файлов. Ко всем этим файлам есть описания, и во многих из них есть интересные нам данные, но начнем мы с самого главного файла — names.nsf. Данный ресурс представляет собой полную базу данных по сотрудникам, их почтовым адресам и по множеству другой полезнейшей информации, такой как: версии ОС пользователей, версии программного обеспечения Lotus Notes и прочие данные. А знаешь, что самое интересное? Этот ресурс на большинстве серверов доступен анонимному пользователю!
Векторов дальнейшей атаки на самом деле огромное множество, учитывая то, что у нас есть такая интересная информация. Вот лишь часть из них.
1. Получив список логинов пользователей, мы можем подбирать пароли к их почтовым ящикам. Кроме того, мы можем узнать, кто из этих пользователей администратор, и подобрать пароль к его аккаунту, что принесет нам большую пользу.
2. Имея на руках почтовую базу сотрудников с именами, должностями и прочей информацией, грех не устроить рассылку и, используя методы социальной инженерии, добиться от пользователей нужных нам действий.
3. Кроме того, в базе names.nsf хранится информация о версии операционной системы пользователя и версии клиентской программы Lotus Notes, которую он использует для получения почты. Это дает нам огромный ресурс для социальной совместно с 0-уязвимостями или старыми багами под уязвимое клиентское ПО. Здесь можно использовать что угодно, от последних дыр в IE (привет Алексею Синцову) и PDF до уязвимостей, обнаруженных в клиентском программном обеспечении Lotus Notes, а точнее — в его ActiveX-компонентах (к примеру, inotes.dll xforce.iss.net/xforce/xfdb/11339), которые доступны в интернете.

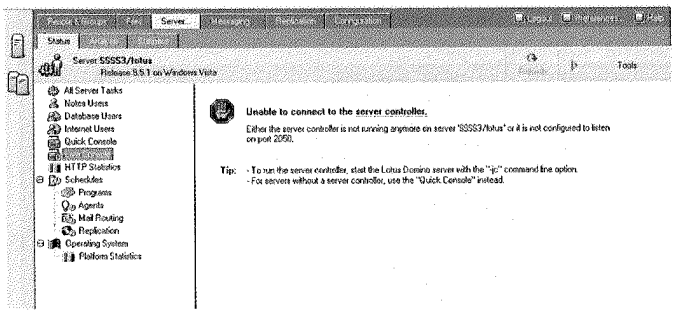
ПОВЫШЕНИЕ ПРИВИЛЕГИЙ

На самом деле озвученная информация — это далеко не все, что можно получить из ресурса names.nsf. Самое сладкое вот в чем — в 2005 году в данном ресурсе была обнаружена уязвимость, которая позволяет читать хэши паролей пользователей системы. Причем уязвимость

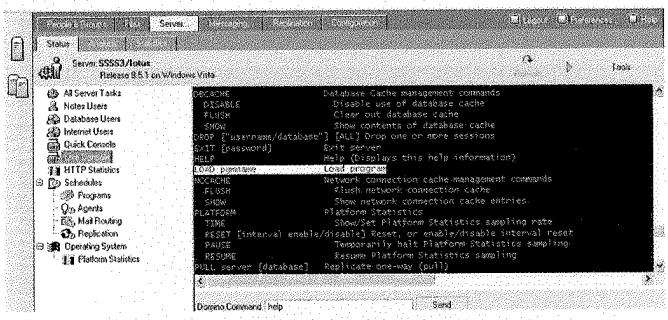
▷ warning

Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несет!

Webadmin.nsf показывает ошибку запуска консоли



Live console в действии – вывод списка возможных команд



банальнейшая. Для получения хэша необходимо перейти на страницу информации о конкретном пользователе и открыть исходный код полученной страницы. Хэш пароля хранится в Hidden поле HTTPPassword или dspHTTPPassword (в зависимости от версии приложения), кроме того, ты можешь встретить два разных алгоритма хэширования, о которых поговорим чуть позже. Что удивительно, уязвимые системы встречаются до сих пор!

Поскольку зачастую количество пользователей исчисляется сотнями или тысячами, то получение хэшей желательно автоматизировать. Но тут не стоит беспокоиться, ибо все уже сделано до нас. Еще в 2007 году был написан эксплойт raptor_dominohash, доступный в Сети, который скачивает хэши всех пользователей, а также утилита DominoHashBreaker, осуществляющая подбор паролей по словарю. Эксплойт лучше переделать, так как он выдает слишком много лишней информации, и ее потом неудобно подавать на вход переборщику паролей. Что касается самого переборщика, то он работает только по словарю и имеет следующий недостаток — мы не знаем, от какого пользователя расшифровался хэш, так как на вход подаются только хэши без привязки к логинам. Таким образом, я бы рекомендовал использовать JohnTheRipper с патчем от jumbo, ибо Джон не только не имеет перечисленных недостатков, но и еще умеет расшифровывать новые «соленые» хэши, чего не умеет DominoHashBreaker.

Итак, как я уже говорил, хэши в Lotus бывают двух видов:

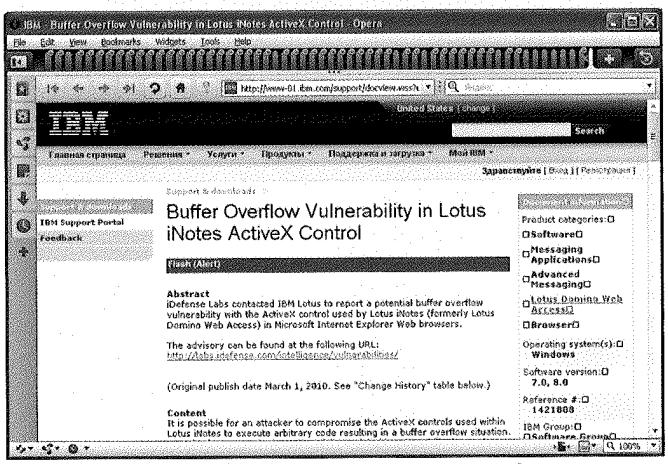
1. Обычные (32 символа в HEX) пример:

```
<input name="$dspPasswordDigest" type="hidden" value
="F05389C37C850260F278FED23334C172">
```

2. С использованием случайных значений (22 символа начинающиеся с G) пример:

```
<input name="$dspHTTPPassword" type="hidden"
value="(GFmjA4YmP9C05vHn09gI)">
```

Для расшифровки обычных хэшей необходимо на вход программе JohnTheRipper подать файл HASH.txt вида:



В клиентских ActiveX естественно есть баги

```
Имя пользователя:хэш
Имя пользователя:хэш
.
.
Имя пользователя:хэш
```

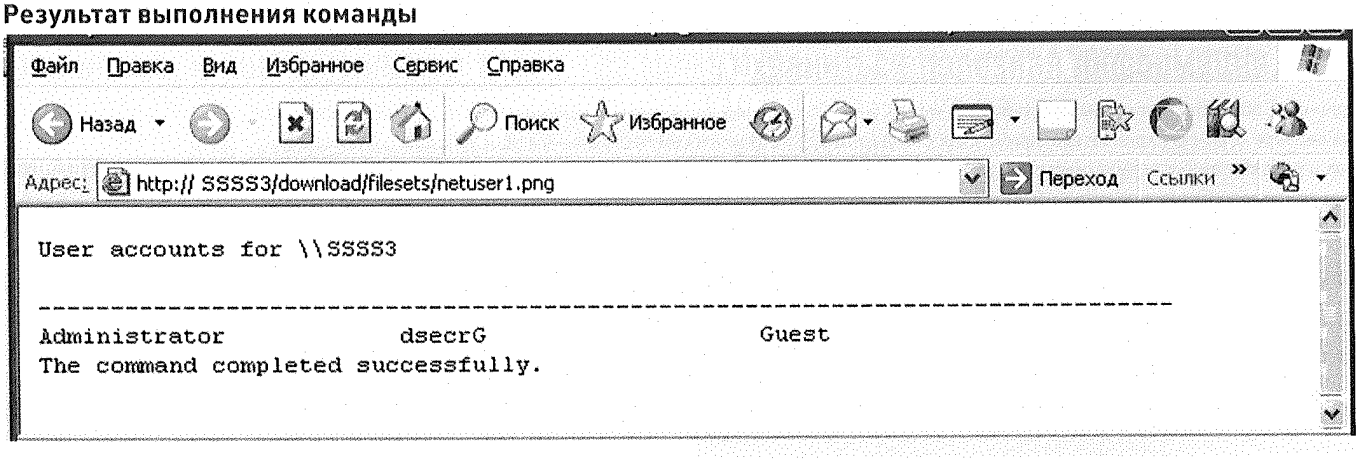
Запускать переборщик необходимо со следующими параметрами:

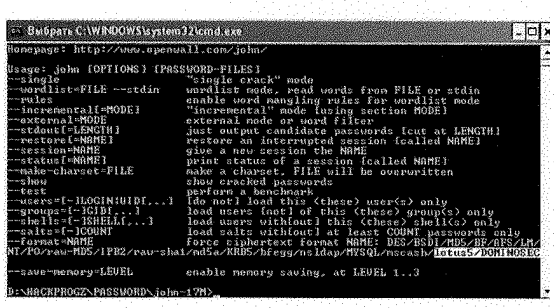
```
./john HASH.txt --format=lotus5
```

Для расшифровки «соленых» хэшей необходимо на вход программе JohnTheRipper подать файл HASH2.txt вида:

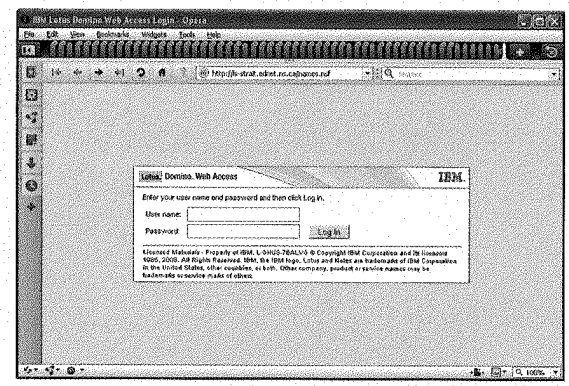
```
Имя пользователя:(хэш)
Имя пользователя:(хэш)
.
.
Имя пользователя:(хэш)
```

Результат выполнения команды





Джон после патча умеет ломать лотусовые пароли



Иногда на names nsf стоит пароль

Запускать переборщик необходимо со следующими параметрами:

```
./john HASH.txt --format=dominosec
```

Вот, собственно, и все, напоследок могу только порекомендовать набрать разных словарей и запустить перебор параллельно брутом и словарями для большей эффективности. В случае успеха, что встречается довольно часто, так как парольные политики в Domino по умолчанию отключены, мы получим список расшифрованных паролей пользователей системы Lotus Domino на Web-доступ. Пусть там будут и не все пользователи, но все же шансы, что из тысячи хоть кто-нибудь расшифруется, достаточно велики.

АДМИНИСТРИРОВАНИЕ

Итак, предположим, что мы расшифровали пароль администратора (если нет, сидим и перебираем дальше :)) — это есть очень хорошо. Теперь перед нами открываются просторы доступа ко всем находящимся на сервере nsf-файлам, которых, как я уже говорил, предостаточно. Интересный ресурс — log.nsf, на нем можно найти и посмотреть все логи доступа к серверу по различным критериям и узнать, к примеру, каким браузером пользуются пользователи. Также интерес представляет catalog.nsf. Доступ к почте каждого сотрудника можно получить, обратившись к директории /mail/логинсотрудника.nsf.
Но самый большой интерес для нас представляет ресурс webadmin.nsf (servername/webadmin.nsf). Это админка Web-сервера Lotus Domino со всеми вытекающими последствиями. Имея доступ к ней, можно создавать, изменять и удалять пользователей, назначать для них группы и выполнять всевозможные административные задачи. Получение административного доступа к системе Lotus Domino практически всегда означает получение доступа к ОС, если не используются расширенные настройки безопасности, такие как: пароль на консоль (иногда встречается) или ограничение прав учетной записи в ОС (на практике крайне редко). Стоит отметить, что в ОС Windows по умолчанию доступ будет получен под учетной записью Local System, так как служба запущена от имени Local System, а в Unix доступ будет получен от имени непривилегированной учетной записи.
Итак, что же предоставляет нам webadmin.nsf? В этом приложении есть различные опции по управлению сервером, в том числе и ряд оболочек для выполнения сервисных команд для репликации и прочих административных задач. Для выполнения сервисных команд можно использовать две различные консоли: Quick Console и Live Console. Но не тут-то было. Эти консоли — не то же самое, что консоль в ОС, так как набор команд там строго определен и заточен под задачи LOTUS.
К нашему счастью, в бизнес-логике этой консоли есть уязвимость, которая заключается в том, что команда Load использует в качестве аргумента не список команд, а реальные исполняемые файлы в системе. То есть, используя небольшой трюк можно запускать исполняемые файлы доступные в директории PATH операционной системы через команду Load (спасибо за данный метод Евгению Киселеву, автору книги «Безопасность IBM Lotus Notes/Domino R7», которую настоятельно рекомендуется почитать тем, кого интересует безопасность Lotus). Рассмотрим эти две консоли поподробнее.

ОБОЛОЧКА LIVE CONSOLE

Наиболее удобная оболочка для выполнения называется Live Console, но, к сожалению, ее использование обусловлено двумя проблемами. Первая проблема заключается в том, что данная консоль не включена по умолчанию и для ее включения необходимо перезагружать сервер, что не очень хорошо. Вторая особенность — данная оболочка работает по своему протоколу с использованием порта 2050, и с большой вероятностью в случае подключения через интернет данный порт будет зафильтрован. Таким образом, данный вариант не является универсальным, так что идем дальше.

ОБОЛОЧКА QUICK CONSOLE

Второй вариант — это использование урезанной версии консоли — Quick Console. Данная консоль имеет неприятную особенность — результат выполнения команды не отображается, таким образом, мы можем выполнять команды только вслепую. Ладно если нам нужно просто выполнить команду, в которой мы уверены, но если нам захочется прочитать содержимое файлов — тут без трюков не обойтись. На самом деле проблема очень похожа на Blind SQL Injection, так что и методы надо применять похожие, только с учетом особенностей.

ПОЛУЧЕНИЕ ДАННЫХ

Давай проанализируем, что мы вообще можем делать в административном интерфейсе, чтобы понять, что из этого нам поможет для получения результатов команд. Первое, что бросается в глаза — это меню Files, где, как хотелось бы верить, мы сможем читать файлы, но и тут нас поджидает неприятная участь. Читать файлы нельзя, можно только делать листинг директорий и видеть имена файлов. И только если у них расширение .nsf.
Первая сумасшедшая идея, которая приходит в голову — это разбивать на строки вывод результата выполнения команды и создавать файлы, в названии которых будет кусок результата выполнения команды, а расширением будет .nsf. Таким хитрым и довольно извращенным способом

links

- dsecrg.ru/pages/pub/ — Исследования из серии «Проникновение в ОС через приложения»
- cybsec.com/vuln/default_configuration_information_disclosure_lotus_domino.pdf — Уязвимость раскрытия информации в Lotus Domono.
- exploit-db.com/exploits/3302 — Эксплойт для автоматизированной скачки хэшей.
- securiteinfo.com/download/dhb.zip — Утилита для подбора паролей по словарю Domino Hash Breaker.
- openwall.com/john/ — Утилита JohnTheRipper для взлома паролей.
- openwall.com/john/contrib/john-1.7.5-jumbo-2.diff.gz — Патч для утилиты JohnTheRipper для взлома паролей в Domino старых и новых версий.
- documents.iss.net/whitepapers/domino.pdf — IBM ISS "Lotus Domino Security" 2002
- seclists.org/pen-test/2008/May/64 — Pentesting Lotus Domino.

Сайт лотуса

мы будем получать информацию о результате работы команды. Для этого необходимо последовательно запустить две команды (спасибо Алексею Синцову за набросанный скрипт):

```
load cmd /c "dir /D /B > sh2kerr.out"
load cmd /c "FOR /F "delims= " %i IN (sh2kerr.out) DO
ECHO > C:\lotus\domino\sh2kerr\"%i".nsf"
```

Первая команда сохраняет результат команды (в нашем примере это команда DIR) в файл sh2kerr.out. Вторая команда разбивает результат вывода первой и создает необходимые файлы. В результате в папке C:\lotus\domino\sh2kerr\ мы увидим множество файлов, в именах которых будет результат выполнения команд.

На самом деле есть способ гораздо проще, но при этом будет вероятность, что он не заработает там, где безопасно расставлены права. На практике мне такого не встречалось, так что можно использовать этот метод практически везде. Метод очень прост и заключается в следующем — необходимо найти директорию, в которую мы можем писать, и которая будет доступна через Web-интерфейс. Такая директория есть по умолчанию в версиях 6.5 и 8.5 (в других она, скорее всего, тоже присутствует, но подтвердить нет возможности). В ОС Windows данная директория в результате установки по умолчанию выглядит следующим образом:

```
C:\Lotus\Domino\data\domino\html\download\filesets\
```

Для того, чтобы обратиться к данной директории через Web-интерфейс, необходимо пройти по следующей ссылке: http://servername/download/filesets. Таким способом можно получить результат выполнения команды на сервере Lotus.

Альтернативный сценарий выполнения команд.

Кроме трюка с Load есть еще один способ выполнения команд — через так называемый планировщик. Находится он в меню Server->Status->Schedules->Programs. Используя этот планировщик, можно также запускать любые команды в ОС.

КЛИЕНТ-СЕРВЕРНОЕ ВЗАИМОДЕЙСТВИЕ

Выше мы рассматривали вопросы безопасности Web-доступа к системе Lotus Domino, но есть еще и другой протокол (NRPC на 1352 порту), по которому можно подключиться к системе. Этот протокол позволяет подключаться к Lotus Domino серверу, используя клиентские программы Lotus Designer (разработчики), Lotus Notes (простые сметные) и Lotus Administrator (спасибо, кэп). Для подключения к серверу клиент должен иметь некое подобие сертификата, в системе Lotus Domino это файл с расширением ID. Помимо этого файла для подключения необходимо иметь и пароль к нему.

Данный пароль никогда не передается по сети и используется для расшифровки ID-файла, а аутентификация происходит уже при помощи расшифрованной информации. Итак, для того, чтобы подключиться к системе с использованием клиентского приложения, нам необходимо получить 2 вещи: ID-файл и пароль к нему. Выглядит сложнее, чем в случае с Web, но не безнадежно.

Для того, чтобы получить ID-файл, можно воспользоваться уязвимостью раскрытия информации в службе Lotus Domino. Уязвимость заключается в возможности получения ID-файла пользователя, в случае, если известен его логин. Логин можно либо подобрать, либо воспользоваться уязвимостью в names.nsf, описанной выше. Второй способ получения ID-файла — попытаться откопать его в том же names.nsf. Очень часто в профиле пользователя, доступном без аутентификации через Web-интерфейс, есть ссылка на скачку его ID-файла.

С первой проблемой разобрались, что же делать со второй? На самом деле тут все банально. Пользователи очень часто ставят простые пароли на ID-файл, так что можно его подобрать, тем более, что для этого есть специализированный софт в количестве, как минимум, 3-х утилит (smashingpasswords.com/3-best-lotus-notes-password-recovery-free-softwares), причем одна из них (IPR) абсолютно бесплатна.

STEP BY STEP HOWTO

Итак, подведем итоги и создадим небольшой гайд по получению доступа к Lotus Domino.

Для получения доступа к серверу выполняем следующие действия:

Если есть Web-доступ:

1. Запускаем утилиту raptor_dominohash и собираем хэши паролей:
./raptor_dominohash 192.168.0.202

2. Сохраняем хэши в формате, приведенном в статье;

3. Запускаем JohnTheRipper и подаем на вход список имен пользователей и хэшей:
./john HASH.txt --format=lotus5

4. В случае расшифровки хэша администратора обращаемся к консоли Web-администрирования по адресу:
http://servername/webadmin.nsf

5. В Quick Console набираем команду, добавляющую в ОС нового пользователя:
load cmd /c net user hacker iamstupid /add

6. Чтобы проверить, выполнилась ли команда, выводим список текущих пользователей и сохраняем вывод команды в файл:
load cmd /c net user > C:\Lotus\Domino\data\domino\html\download\filesets\1.txt

Для просмотра результата выполненной команды обращаемся по следующей ссылке:
http://servername/download/filesets/1.txt , и, в случае успеха, видим подтверждение выполненной команды;

7. Если не получилось, пробуем выполнить команду через Program.

Если есть NRPC-доступ:

1. Берем список пользователей из names.nsf (или подбираем) и пытаемся получить ID;

2. В случае получения ID пытаемся расшифровать пароль при помощи утилит указанных в статье;

3. В случае успеха пытаемся подключиться при помощи Lotus Administrator, а далее начинаем с пункта 5 предыдущего варианта.

И ЧТО ПОТОМ?

В статье я попытался представить основные способы получения шелла на сервере через уязвимости и недостатки конфигурации Lotus Domino. Ряд вопросов, таких как: подробности получения ID-файла, прочие критичные nsf-файлы и ошибки типа xss в Web-доступе, получение доступа к другим серверам через репликацию и прочие аспекты безопасности, описание которых выходит за рамки данной статьи, я оставлю тебе для самостоятельного изучения. Старательно используй собранные ссылки на ресурсы, приведенные в этой статье, а также посещай сайт нашей исследовательской лаборатории DSecRG.ru, и, если есть желание, присоединяйся (research@dsec.ru).