Подписание зоны с помощью OpenDNSSEC - часть 1

1. Инициализируйте программу "Hardware Security Module"

    Начните с получения прав администратора

    ```
    $ sudo -s
    #
    ```

    ```
    # softhsm --init-token --slot 0 --label OpenDNSSEC
    ```

    (ответьте '1234' на оба вопроса ниже):

    ```
    The SO PIN must have a length between 4 and 255 characters.
    Enter SO PIN: ****
    The user PIN must have a length between 4 and 255 characters.
    Enter user PIN: ****
    The token has been initialized.
    ```

    ```
    # softhsm --show-slots
    ```

    Создайте файлы конфигурации для OpenDNSSEC, скопировав
    примеры конфигурации, входящие в комплект поставки:

    ```
      # cd /usr/local/etc/opendnssec
      # cp kasp.xml.sample kasp.xml
      # cp conf.xml.sample conf.xml
      # cp addns.xml.sample addns.xml
      # cp zonelist.xml.sample zonelist.xml
      # chmod 644 *xml
    ```

2. Поменяйте стратегию по умолчанию с использования NSEC3 на использование NSEC

    Отредактируйте /usr/local/etc/opendnssec/kasp.xml

    Найдите следующий раздел, уберите все строки от <NSEC3> до </NSEC3>

    ```
    <NSEC3>
        <!-- <OptOut/> -->
        <Resalt>P100D</Resalt>
        <Hash>
            <Algorithm>1</Algorithm>
            <Iterations>5</Iterations>
            <Salt length="8"/>
        </Hash>
    </NSEC3>
    ```

    ... и замените их на эту строку:

    ```
    <NSEC/>
    ```

    Сохраните файл и выйдите из редактора.

    Также, установите правильный путь к libsofthsm.so в conf.xml:

    Поменяйте

```
<Module>/usr/local/lib/libsofthsm.so</Module>
```

на

```
<Module>/usr/local/lib/softhsm/libsofthsm.so</Module>
```

В том же файле, найдите строку:

```
<Datastore><SQLite>/usr/local/var/opendnssec/kasp.db</SQLite></Datastore>
```

Удалите ее, и добавьте:

```
<Datastore>
    <MySQL>
        <Host port="3306">localhost</Host>
        <Database>opendnssec</Database>
        <Username>root</Username>
        <Password></Password>
    </MySQL>
</Datastore>
```

3. Запустите MySQL и создайте базу данных

Отредактируйте /etc/rc.conf, и добавьте:

```
mysql_enable="YES"
```

Сохраните файл и выйдите из редактора, затем запустите:

```
# service mysql-server start
```

Вы должны увидеть:

```
Starting mysql.
```

Создайте базу данных:

```
# echo "create database opendnssec" | mysql
```

4. Инициализируйте KSM

```
# ods-ksmutil setup

*WARNING* This will erase all data in the database; are you sure? [y/N] y
Enter password:
```

Просто нажмите ВВОД вместо ввода пароля.  Вы увидите:

```
    zonelist filename set to /usr/local/etc/opendnssec/zonelist.xml.
    kasp filename set to /usr/local/etc/opendnssec/kasp.xml.
    Repository SoftHSM found
    No Maximum Capacity set.
    RequireBackup NOT set; please make sure that you know the potential problems of
using keys which are not recoverable
    INFO: The XML in /usr/local/etc/opendnssec/conf.xml is valid
    INFO: The XML in /usr/local/etc/opendnssec/zonelist.xml is valid
    INFO: The XML in /usr/local/etc/opendnssec/kasp.xml is valid
    Policy default found
```

5. Установите копию неподписанной зоны (OpenDNSSEC будет ее подписывать)

Ранее мы сделали бэкап нашей зоны, прежде чем она была подписана BIND9. Сейчас мы используем эту копию и сделаем ее доступной для OpenDNSSEC.

```
# cd /etc/namedb/master
# cp mytld.backup /usr/local/var/opendnssec/unsigned/mytld
```

Увеличьте серийный номер в файле зоны, так что он отражает реальность (YYYYMMDDXY).

6. Добавьте зону в базу данных OpenDNSSEC:

```
# ods-ksmutil zone add --zone mytld

zonelist filename set to /usr/local/etc/opendnssec/zonelist.xml.
Imported zone: mytld
```

7. Запустите OpenDNSSEC!

Добавьте следующее в /etc/rc.conf

```
opendnssec_enable="YES"
```

Сохраните файл и выйдите из редактора.

Теперь, запустите сервис:

```
# service opendnssec start
```

Вы увидите:

```
Starting enforcer...
OpenDNSSEC ods-enforcerd started (version 1.4.3), pid 2923
Starting signer engine...
OpenDNSSEC signer engine version 1.4.3
Engine running.
```

```
# ps ax | grep ods

41588  ??  SsJ    0:00.11 /usr/local/sbin/ods-enforcerd
41593  ??  SsJ    0:00.07 /usr/local/sbin/ods-signerd
```

8. Убедитесь, что зона подписана

```
# ls -l /usr/local/var/opendnssec/signed

-rw-r--r--  1 root  wheel  2621 Feb 19 09:10 mytld
```

Посмотрите содерижимое зоны - обратите внимание на идентификаторы ключей KSK и ZSK.

Если по какой-то причине вы не видите этого файла в каталоге /usr/local/var/opendnssec/signed/, заставьте подписанта подписать зону:

```
# ods-signer sign mytld
```

9. Немного размышлений

Хорошо, теперь зона подписана OpenDNSSEC - обратите внимание, что зона была подписана, но вы не выполняли никаких команд для создания ключей.

Показать ключи под управлением OpenDNSSEC:

```
# ods-ksmutil key list
```

```
Keys:
Zone:                           Keytype:      State:    Date of next transition:
mytld                           KSK           publish   2014-03-21 04:25:30
mytld                           ZSK           active    2014-03-21 04:32:30
```

Обратите внимание, что два ключа были созданы OpenDNSSEC на лету.

Но BIND пока еще подгружает зону, которая была подписана ранее (или вручную или используя встроенное подписание) - нельзя ли просто изменить конфигурацию в named.conf и указать на зону подписанную OpenDNSSEC?

Какой KSK сейчас используется? Какие записи DS были опубликованы в родительской зоне?

Смогут ли системы разрешения имен проверять подписи в зоне, подписаной OpenDNSSEC? Почему нет? Что вам нужно сделать, чтобы все заработало? (На этот вопрос есть несколько возможных ответов)

Если вас не заботит проблема валидации, вы можете продолжить выполнять оставшуюся часть этой лабораторной работы.

10. Инструктируйте BIND подгрузить новую зону

Измените /etc/namedb/named.conf, поменяв определение зоны для "mytld", так что она выглядит примерно следующим образом (УДАЛИТЕ auto-dnssec и т.д.):

```
zone "mytld" {
    file "/usr/local/var/opendnssec/signed/mytld";  // <--- измените путь
    type master;
    key-directory "/etc/namedb/keys";   // <--- Удалите если наличествует
    auto-dnssec maintain;               // <--- Удалите если наличествует
    inline-signing yes;                 // <--- Удалите если наличествует
};
```

Теперь, BIND работает как "пассивный" DSN-сервер, который не подписыват зону - он просто обслуживает зону, подписанную при помощи OpenDNSSEC.

Перезапустите named:

```
# service named restart
```

Проверьте логи в /etc/namedb/log/general и убедитесь в том, что зона подгружается правильно.

Сейчас валидация теми, кто попытается получить данные в вашей зоне, скорее всего не будет успешна. Подождите несколько минут и попробуйте запросить какую-нибудь запись из вашей зоны:

```
    # dig @127.0.0.1 www.mytld +dnssec
```

    На что вы обратили внимание?

11. OpenDNSSEC, перезапускающий BIND

    Что хорошо, вы можете настроить OpenDNSSEC, чтобы он говорил BINDу перезагрузить зону, когда она подписывается.  Таким образом, перегрузка вручную не понадобится.

    Чтобы это сделать, измениете /usr/local/etc/opendnssec/conf.xml

    Найдите строчки:

```
<!--
                <NotifyCommand>/usr/sbin/rndc reload %zone</NotifyCommand>
-->
```

    ... и удалите комментарии (строки '<!--' and '-->') до и после.

    Сохрание файл, и перезапустите OpenDNSSEC:

```
    # ods-control stop
    ...
    # ods-control start
```

12. Эскпортируйте DS, готовый для закачки:

    Теперь проверьте состояние KSK:

```
    # ods-ksmutil key list
```

    Обратите внимание на состояние, в котором находится KSK.

    Если он до сих пор в состоянии (publish) (см. https://wiki.opendnssec.org/display/DOCS/Key+States#KeyStates-Publish для детального описания), то ключ, с точки зрения OpenDNSSEC, не готов к использованию, поскольку не прошло достаточно времени для его распространения.

    Вы все еще можете экспортировать запись DS, созданную из KSK:

```
    # ods-ksmutil key export --zone mytld --ds --keystate publish
```

    Обратите внимание на предупреждение!

```
WARNING: No active or ready keys seen for this zone. Do not load any DS records to
the parent unless you understand the possible consequences.
```

    Хорошо, давайте сохраним DS в файле, который мы потом сможем закачать:

```
    # ods-ksmutil key export --zone mytld --ds --keystate publish >/tmp/dsset-
mytld.
```

13. Закачайте DS на сервер

    Если вы не используете web интерфейс:

```
    # scp /tmp/dsset-mytld. sysadm@a.root-servers.net:
```

14. Дайте знать администратору!

    Попросите администратора корневой зоны добавить новую запись DS,
    и посмотрите, сколько времени пройдет прежде чем валидация начнет
    опять работать для вашей зоны.

    ... или, если вы используете web интерфейс:

    Залогиньтесь на https://rzm.dnssek.org и исправьте записи DS,
    проверив DS-записи с "глазами", отмечая их и потом нажимая "Update".
    После нескольких минут для обновления кэшей, система разрешения
    имен должна валидировать.  Если у вас не исчезают проблемы,
    попросите преподавателя очистить кэши.

15. Что происходит с состоянием ключа?

    Почему ключ находится в состоянии "Publish"?  Отчего OpenDNSSEC
    не жаждет разрешить нам использовать ключ сразу?

    Was it a good idea to upload the DS already ?
    Было ли это хорошей мыслью, когда мы закачали DS сразу?

    Если вы подождете достаточно долго, вы увидите:

```
Keys:
Zone:                           Keytype:      State:    Date of next transition:
mytld                           KSK           ready     waiting for ds-seen
mytld                           ZSK           retire    2014-03-21 07:50:38
mytld                           ZSK           active    2014-03-21 07:54:38
```

    На самом деле, нам следовало подождать до тех пор пока ключ не
    перешел бы в состояние "ready", и только потом публиковать DS!

    Почему?  Существовал риск того, что информация о зоне была не полностью
    распространена (слейвы и кэши).  Только после того как ключ отмечен
    как "ready", становится безопасным закачивать DS.  OpenDNSSEC использует
    параметры в стратегических настройках (kasp.xml) чтобы определить
    эти временные интервалы.

16. Дать знать OpenDNSSEC о том, что DS появлися в родительской зоне

    Когда вы увидели DS в родительской зоне, и KSK находится в состоянии
    "ready", вы можете дать об этом знать OpenDNSSEC.

    # ods-ksmutil key list -v

```
Keys:
Zone:                           Keytype:      State:    Date of next transition
(to):  Size:   Algorithm:  CKA_ID:                            Repository:
Keytag:
mytld                           KSK           ready     waiting for ds-seen
(active)   2048    8           0c4f577032e04e2eb34163382a4524d7  SoftHSM
44096
mytld                           ZSK           active    2014-03-21 07:54:38
(retire)   1024    8           bbd9b3e14c3cbb0517d49f79985916bd  SoftHSM
57634
mytld                           ZSK           publish   2014-03-21 09:02:55 (ready)
1024    8           7982538186c1b77afe84e6875f3c7bda  SoftHSM
```

51991

-v дает вам идентификаторы ключей, которые вам понадобятся на следующем шаге.

Запишите идентификатор ключа KSK, находящегося в состоянии `ready`.

Теперь, выполните:

```
# ods-ksmutil key ds-seen --zone mytld --keytag 44096
```

... где 44096 - идентификатор KSK из предыдущего примера.

Вы увидите:

```
Found key with CKA_ID 0c4f577032e04e2eb34163382a4524d7
Key 0c4f577032e04e2eb34163382a4524d7 made active
Notifying enforcer of new database...
Performed a HUP ods-enforcerd
```

Теперь, посмотрите ключи снова:

```
# ods-ksmutil key list
```

Note that the KSK is now marked active.
Обратите внимание на то, что KSK теперь отмечен как "активный".