Упражнение: Обновление ключа вручную

ЗАДАЧА

Мы собираемся обновить ZSK для зон, которые мы только что подписали.

ПОЖАЛУЙСТА запишите идентификаторы ключей KSK/ZSK на листке бумаги,
чтобы не забыть, какой ключ выполняет какую задачу.

НАПОМИНАНИЯ

- мы храним наши ключи в /etc/namedb/keys/

- там у нас сейчас хранится две пары ключей, одна пара для ZSK и одна для KSK. Каждая пара представлена двумя файлами, один заканчивается на ".key" (открытый ключ), и другой заканчивается на ".private" (закрытый ключ)

- в корневой зоне есть набор записей DS, соответствующий нашему KSK

ОБНОВЛЕНИЕ ZSK

1. Посмотрите на уже существующие ключи. Запишите имена файлов,
в которых хранится текущий ZSK и текущий KSK.

```
$ cd /etc/namedb/keys/
$ ls K*
```

2. Создайте новый ZSK, которым мы заменим старый.

```
$ sudo dnssec-keygen -a RSASHA256 -b 1024 -n ZONE mytld
```

(заменяя mytld именем вашей зоны)

Эта команда выведет что-то вроде:

```
Kmytld.+008+45000
```

Убедитесь, что все файлы ключей могут читаться процессом named:

```
$ sudo chown bind K*
$ sudo chmod u+r K*
$ ls
```

Теперь у вас должна быть третья пара ключей в ключевом каталоге. Если вы проверите содержимое DNSKEY, вы должны увидеть, что поле флагов равно 256 (то есть это ZSK, а не KSK). Запишите имя файла с новым ZSK.

3. Посмотрите на теперешний набор DNSKEY.

```
$ dig mytld dnskey +multi
```

Ваша зона должна содержать один KSK и один ZSK (проверьте флаги - 267/256 - для того чтобы отличить один от другого).

Нам нужно добавить новый ключ в зону, так что он будет в ней во время следующего подписания. В конец файла /etc/namedb/master/mytld, ДОБАВЬТЕ

новый ключ:

    $include "/etc/namedb/keys/Kmytld.+008+45000.key";

    Увеличьте серийный номер.

    Сохраните файл и выйдите из редактора

4. Переподпишите вашу зону, чтобы новый ZSK был подписан, при этом мы НЕ
   будем подписывать зону используя новый ZSK - пока мы только хотим, чтобы
   новый ZSK был подписан текущим ZSK. Это называется "предварительная
   публикация".

  $ cd /etc/namedb/keys
  $ sudo dnssec-signzone -o mytld -k Kmytld.+008+52159 ../master/mytld Kmytld.
+008+51333

  (метка и идентификатор ключа берется из предыдущей лабораторной работы по
  подписанию вручную)

  В примере выше, обратите внимание на то, что мы используем текущий ZSK
  для подписания, а *НЕ* новый - это нужно для того, чтобы убедиться
  в том, что dnssec-signzone не пытается подписывать обоими ZSK.
  Если такое случится, не произойдет ничего "страшного", просто
  размер зоны разбухнет в два раза!

  Таким образом, мы говорим dnssec-signzone какие именно ключи использовать
  во время обновления, ИМЕННО для того, чтобы управлять моментами, когда
  новый ключ добавляется, когда он используется для подписей, и когда
  он изымается из обращения.

  Вывод команды выше должен быть:

Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 1 stand-by, 0 revoked
mytld.signed

  Обратите внимание на ZSK: 1 active, 1 stand-by

5. Посмотрите, что эта операция сделала с зоной.

  $ sudo rndc reload mytld
  $ dig @10.20.X.1 mytld dnskey
  $ dig @10.20.X.1 mytld dnskey +dnssec
  $ dig @10.20.X.1 mytld soa +dnssec

Ваша зона теперь должна содержать один KSK и два ZSK; оба ZSK должны
быть в наборе записей DNSKEY, который должен быть подписан при
помощи KSK.

ОДНАКО, запись SOA (и другие наборы записей в зоне) должны быть ТОЛЬКО подписаны
единожды, при помощи старого ZSK. И набор DNSKEY должен показывать все три
ключа (1 KSK, 2 ZSK). Это называется "предварительная публикация".

Теперь, нам стоит в принципе подождать 2 раза по TTL до появления
обоих ZSK во всех кэшах (по умолчание это 120 секунд, или 2 минуты,
в нашей лабораторной, но значения будут другими "в настоящей жизни").
В любом случае, давайте подождем по крайней мере 2 минут прежде чем мы

осуществим подписание с новым ZSK вместо старого ZSK.

После 2 минут, спросите соседа о том, может ли он запросить DNSKEY для вашего домен. Они могут проверить кэш класса (10.20.0.230), а также, если они его настроили, из собственный кэш.

Опять-таки, команда для запроса ключей будет:

```
  $ dig mytld dnskey
```

После получения уверенности в том, что "весь интернет" (весь класс) может видеть оба ключа, мы может подписать зону новым ZSK.

6. Осуществите полписание новым ZSK.

   Помните, у нас сейчас 3 ключа - в нашей зоне есть:

```
        $include "/etc/namedb/keys/Kmytld.+008+52159.key"; // KSK
        $include "/etc/namedb/keys/Kmytld.+008+51333.key"; // ZSK мы уберем
        $include "/etc/namedb/keys/Kmytld.+008+45000.key"; // новый ZSK
```

   Увеличьте серийный номер. Затем:

```
   $ cd /etc/namedb/keys
   $ sudo dnssec-signzone -o mytld -k Kmytld.+008+52159 ../master/mytld Kmytld.
+008+45000
```

... Обратите внимание, что теперь мы используем 45000 (второй ZSK) для подписи, а не 51333 как раньше

Теперь, перегрузите зону для распространения изменений

```
   $ sudo rndc reload mytld
```

При помощи dig проверьте (как в шаге 5), что вы видите только ОДНУ подпись для ваших наборов записей - что означает что мы подписываем только ОДНИМ ZSK - вам нужно опять-таки подождать время TTL, прежде чем вы можете убрать старый ZSK.

7. Теперь вы должны заметить, используя dig как в шаге 5, что мы подписали только лишь одним ключом

```
   $ dig www.mytld +dnssec
```

Также проверьте, что СТАРЫЙ ZSK все еще опубликован в наборе записей DNSKEY:

```
   $ dig mytld dnskey
```

Вы по-прежнему должны видеть три ключа.

8. Изымите старый ZSK из обращения.

После двухминутного ожидания (120с), уберите старый ZSK:

```
  $ cd /etc/namedb/master/
```

  Отредактируйте файл зоны и добавьте знак комментария (';') впереди старого ZSK (проверьте и перепроверьте, какой ключ закомментировать!)

```
  $ sudo ee mytld

$include "/etc/namedb/keys/Kmytld.+008+52159.key";  // KSK
;$include "/etc/namedb/keys/Kmytld.+008+51333.key"; // ZSK (закомментирован)
$include "/etc/namedb/keys/Kmytld.+008+45000.key";  // новый ZSK
```

Увеличьте серийный номер.

Теперь переподпишите зону, и обратите внимание что мы специфически НЕ указываем ZSK, который мы закомментировали:

```
  $ cd /etc/namedb/keys
  $ sudo dnssec-signzone -o mytld -k Kmytld.+008+52159 ../master/mytld Kmytld.
+008+45000
  $ sudo rndc reload mytld
  $ tail /etc/namedb/log/general
```

9. Точно как в шаге 5, проверьте что подписи по прежнему работают, и что СТАРЫЙ ZSK более не находится в наборе записей DNSKEY.

   Также, убедитесь что записи RRSIG (dig +dnssec soa mytld) в вашей зоне показывают идентификатор нового ключа ZSK.

   Работает ли ваш домен сейчас? :)