

BIND: ЗАЩИТА СКАЧИВАНИЯ

Мы собираемся ограничить скачивание ваших зон так, что только ваши слейвы могут получать копии зон.

Замечание: если группа преподавателя (например, группа 0) является слейвом для вашего домена, то "партнер", упомянутый ниже - это преподаватель, ответственный за группу 0.

Защита, основанная на списках контроля доступа

Для начала, мы включим список контроля доступа, основанный на IP адресе -- на машине AUTH1:

1. Отредактируйте файл /etc/namedb/named.conf, и в разделе "options", определите, кому разрешено скачивание вашей зоны.

```
allow-transfer { 127.0.0.1; ::1; YOUR_OWN_IP; myslaves; };
```

... замените "YOUR_OWN_IP" на IP адрес вашей машины :)

Теперь нам нужно определить ACL "myslaves". Чтобы достичь этого, ПОСЛЕ раздела "options" (найдите символы '};' в конце этого раздела), добавьте что-то вроде этого:

(Если слейв для вашего домена "MYTLD" - auth1.grp25, например)

```
acl myslaves { 10.20.25.1; }; // ACL с IP мастера группы 25
```

Это означает "myslaves является списком доступа состоящим из IP-адреса 10.20.25.1."

Если вы также используете NSD, вам также будет нужно добавить IP вашего вторичного сервера в вашей сети в ACL (это применимо только если вы сконфигурировали NSD в качестве вторичного сервера в вашей группе. Если это не так, просто пропустите этот шаг)

```
acl myslaves { 10.20.25.1; 10.20.X.2; }; // ACL с IP мастера группы 25 и ваш  
вторичный NSD 10.20.25.2.
```

Замечание: вводите правильные значения! Вы должны указать IP машины, которая является вашим вторичным сервером в классе!

2. Перезапустите named

```
$ sudo service named restart
```

3. Убедитесь, что вы не поломали скачивание зоны, попросив вашего партнера-слейва выполнить скачивание зоны с ВАШЕЙ машины.

С их сервера:

```
$ dig @auth1.grpX.dns.nsrc.org MYTLD axfr
```

Убедитесь, что это по-прежнему работает.

4. Теперь попробуйте попросить кого-нибудь другого в классе, чей сервер НЕ упомянут в ACL, попытаться выполнить такую же команду скачивания, как было указано выше.

Q: Получилось ли у них это сделать?

Q: Что вы видите в логге /etc/namedb/log/general ?
Что вы видите в логге /etc/namedb/log/transfers ?

Защита, основанная на TSIG KEY

Вместо использования IP-адресов, мы теперь будем пользоваться криптографическими ключами для удостоверения прав на скачивание зоны -- это использует TSIG, механизм, с помощью которого коммуникация между мастером и слейвом будет удостоверяться при использовании такого ключа.

1. Выполните:

```
$ cd /tmp/  
$ sudo dnssec-keygen -a HMAC-MD5 -b 128 -n HOST mydomain.key
```

Вы увидите что-то вроде такого:

Kmydomain.key.+157+32373 (последнее число будет другим)

Два файла были созданы:

```
$ ls -l K*
```

```
Kmydomain.key.+157+32373.key  
Kmydomain.key.+157+32373.private
```

2. Посмотрите содержимое файла с закрытым ключом:

```
$ cat Kmydomain.key.+157+32373.private
```

Вы увидите что-то похожее на:

```
Private-key-format: v1.2  
Algorithm: 157 (HMAC_MD5)  
Key: tHTRSKKrmYgMpnzNCf2IRA==  
Bits: AAA=
```

... "Key:" здесь - важная для нас информация, поэтому скопируйте "tHTRSKKrmYgMpnzNCf2IRA==", но конечно не тот вариант что вверху, а тот, который находится в ВАШЕМ файле :)

Мы его используем на следующих шагах.

3. Измените ваш named.conf

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

Отредактируйте файл, и измените блок allow-transfer, так что он выглядит следующим образом:

```
options {  
    ...
```

```
allow-transfer { 127.0.0.1; ::1; }; // myslaves убраны!
...
};
```

Замечание: мы убрали "myslaves"

Теперь, после раздела "options", в конце файла, добавьте декларацию ключа

```
key "mydomain-key" {
    algorithm hmac-md5;
    secret "tHTRSKKrmYgMpnzNCf2IRA=="; // Здесь ваш НАСТОЯЩИЙ ключ!
};
```

Не забудьте поменять "mydomain" на имя вашего домена!

Изменение определения вашей зоны:

```
zone "MYTLD" {
    type master;
    file "/etc/namedb/master/mytld";

    allow-transfer { key mydomain-key; };    // <-- добавьте это!
};
```

Как вы можете увидеть, мы добавили блок "allow-transfer", разрешая скачивание зоны держателям ключа "mydomain-key".

Замечание: блок allow-transfer теперь находится ВНУТРИ определения зоны, а не глобально внутри раздела "options" -- BIND может управлять правами на скачивание либо глобально, либо отдельно для индивидуальной зоны. Мы могли бы разрешить скачивание ГЛОБАЛЬНО (для всех зон), если бы мы оставили блок allow-transfer в главном разделе "options".

4. Перезапустите named

```
$ sudo service named restart
```

5. Попробуйте скачать зону с ДРУГОЙ машины -- попросите ваших соседей сделать:

```
$ dig @10.20.XX.1 MYTLD axfr
```

Загляните в /etc/namedb/log/general и в /etc/namedb/log/transfers

Q: На что вы обратили внимание?

6. Потом, попросите их попытаться снова с ключом:

```
$ dig @10.20.XX.1 axfr mydomain -y mydomain-key:tHTRSKKrmYgMpnzNCf2IRA==
```

Q: Что произошло теперь?

Загляните в логи снова, особенно в /etc/namedb/log/transfers

7. На СЛЕЙВЕ вашего партнера (ваш вторичный сервер - опять-таки, это может быть ваш преподаватель, если он обеспечивает вторичный сервис для вашего домена).

Сначала попросите вашего партнера удалить их копию вашей зоны:

- Пусть он уберет зону из /etc/namedb/slave/MYTLD --
помните, это все на машине вашего партнера-СЛЕЙВА:

```
$ sudo rm /etc/namedb/slave/MYTLD
```

- Попросите его перезапустить named

```
$ sudo service named restart
```

Вместе с ним, проверьте, что зона ушла, А ТАКЖЕ что его сервер не может ее получить опять.

Q: Что вы видите в логах (transfers и general) на МАСТЕРЕ (auth1)?

Q: Что вы видите в логах (transfers и general) СЛЕЙВА?

8. Все еще на СЛЕЙВЕ (если преподаватель обеспечивает вторичный сервис, он выполнит этот шаг)

Найдите раздел для зоны:

```
zone "MYTLD" {  
    type slave;  
    masters { 10.20.XX.1; };  
    file "slave/mydomain.dns";  
};
```

... и добавьте ключ, и блок, который сообщает серверу, какой ключ использовать при связи с мастером, "10.20.XX.1":

```
key mydomain-key {  
    algorithm hmac-md5;  
    secret "tHTRSKKrmYgMpnzNCf2IRA==";  
};  
server 10.20.XX.1 {           // здесь вы помещаете IP ВАШЕГО мастера  
    keys { mydomain-key; };  
};
```

9. Перезапустите named

```
$ sudo service named restart
```

На СЛЕЙВЕ:

Q: Появилась ли зона "MYTLD" в каталоге slave/ ?

Q: Что вы видите в логах (transfers и general) СЛЕЙВА?

На МАСТЕРЕ:

Q: Что вы видите в логах (transfers и general) на МАСТЕРЕ (auth1)?

Видите ли вы, в общем случае, пользу использования ключей вместо IP ACL?

Дополнительный раздел, если вы обеспечиваете вторичный сервис сами:

10. Теперь, сделайте то же самое для вашего сервера NSD ("auth2")

... поскольку вы запретили список доступа по IP, ваш AUTH NSD сервер неспособен скачать зону!

Почитайте документацию для NSD (man nsd.conf) если вы не уверены, как указать ключ в NSD для скачивания зоны. Измените определение зоны для MYTLD, так что оно теперь использует KEY вместо NOKEY для скачивания зоны с вашего МАСТЕРА (auth1).

После того, вам будет нужно выполнить "nsdc restart". Скачивается ли зона? Не забудьте проверить логи также и на МАСТЕРЕ (auth1)!

Дополнительный раздел, если вы используете Swatch для мониторинга логов:

11. Если вы настроили Swatch в предыдущем упражнении, сделайте так, что он сообщает, когда видит запрещенное скачивание зоны:

Отредактируйте /usr/local/etc/swatch.conf, и добавьте новый раздел -- не забудьте использовать TAB вместо пробела в начале строк:

```
- - - - - линия отреза - - - - -  
  
watchfor /client ([0-9.:]+)\D\d+: zone transfer '(.*)\./.XFR\IN' denied$/  
    mail=sysadm,subject=Denied AXFR for zone '$2' from $1  
    threshold type=limit,count=1,seconds=600
```

```
- - - - - линия отреза - - - - -
```

12. Остановите Swatch

```
$ ps ax | grep swatch
```

Найдите идентификатор процесса (число слева), и прибейте его:

```
$ sudo kill PID_OF_SWATCH
```

Перезапустите swatch (получите права администратора используя команду sudo -s)

```
$ sudo -s  
# /usr/local/bin/swatch -c /usr/local/etc/swatch.conf --tail-  
file=/etc/namedb/log/general --daemon  
# exit  
$
```

Замечание: Почему вы говорите swatch смотреть в лог "general" ?

Если вы помните предыдущую лабораторную о логировании, мы сконфигурировали BIND логировать категорию безопасности в канал "general". Поэтому нам нужно мониторить файл /etc/namedb/log/general.

13. Выполните еще раз скачивание зоны как на шаге 4 (с другой машины) и посмотрите, получает ли пользователь sysadm письмо, когда вы пытаетесь скачать зону:

```
$ mutt -f /var/mail/sysadm
```

Попробуйте скачивание еще пару раз в течение минуты.

Q: Сколько писем вы получили? Почему?