Автор:
23.12.10 18:31 -

Немного о ssh.

Самое страшное, что может быть в жизни админа, это когда взломщик может получить доступ к шеллу. Поэтому ssh должен быть защищен в первую очередь и с особой тщательностью. Конфиг находится в /**etc**/**ssh**/**sshd_config** разберем некоторые опции:

```
# По умолчанию установлен порт 22.
# Но будет весьма неплохо переставить на другой порт, например, 2200,
# таким образом, взломщики с тупым перебором ip-адресов, будут отдыхать,
# а таких большинство.
Port 2200

# Использовать только протокол ssh v.2. Ибо первый протокол - старьё.
Protocol 2

# Ни в коем случае root не должен подключаться удаленно.
PermitRootLogin no

# Объяснять не надо
PermitEmptyPasswords no

# Интересный параметр MaxStartups. В данном случае, мы устанавливаем,
# что в соединении отказывается в 10% случаев, при трех незавершенных
# подключениях. Не очень удобно самому, значительно неудобнее брутфорсеру.
MaxStartups 0:10:3

# Очень полезная опция AllowUsers.
# Можно через пробел указать кому вообще можно подключаться по ssh.
# Таким образом, мы защищаем себя от случайных пользователей из /etc/passwd.
# Особенно актуально, когда в системе зарегистрировано много пользователей,
# например, для почтовых или ftp подключений.
# Можно указать с каких хостов пользователь может подключаться.
AllowUsers clown chainik test@192.168.0.15
```

Но все это интересно с точки зрения безопасности, например, перевешивание порта несёт некоторые неудобства (надо подключаться **ssh server -p 2200**), зато прекрасно освобождает /var/log/auth.log от мусорных попыток подключиться брутфорсерам. Но ssh - это не только telnet по защищенному соединению. Есть еще очень любопытные фичи в конфиге.

AllowTcpForwarding yes

По умолчанию установлена в **No**. После установки в **YES** и перезапуска демона ssh (например так: **/etc/rc.d/sshd restart**) можно организовать тунель через этот компьютер. Лично я использую эту возможность для удаленного подключения к своему рабочему компьютеру, стоящему за офисным шлюзом, из дома, или очень удобно для подключения к виндовому компьютеру, за этим фаерволом.
Например:

user@localhost% ssh dark@work-gateway.ru -L 127.0.0.1:3388:192.168.0.2:3389

Небольшое описание:
work-gateway - удаленный (для дома) офисный шлюз
127.0.0.1:3388 - на свой собственный компьютер мы биндим подключение на порт 3388 (не всегда срабатывает указание того же порта, что и на машине за шлюзом)
192.168.0.2:3389 - виндовая машина, находящаяся в офисе за шлюзом. Порт 3389, думаю, все знают, что означает.
После выполнения этой команды и успешного установления туннеля можно смело подключаться на localhost порт 3388, например, так:

user@localhost% rdesktop -g 1024x768 127.0.0.1:3388

и вуа-ля! мы на машине за шлюзом. Преймущества такого подключения очевидны:

1. Мы не светим виндовый RDP порт. Его вообще нет для сканирующих.
2. Поключаемся по защищенному туннелю. Я, конечно, понимаю что RDP тоже шифруется, но ssh я как-то доверяю больше.
3. Не надо менять правила фаервола.
4. Можно обеспечить подключение к удаленному внутренниму серверу даже с виндовых машин через тот же putty или ssh tunnel с использованием сертификатов для определенной группы пользователей, даже выставив им nologin. То есть шелл они получить не смогут, зато обеспечить подключение к внутреннему серверу по сертификату - пожалуйста. С моей точки зрения, вариант лучше чем vpn, когда надо ограничить пользователя не сетью, а лишь одной машиной.
Понятно, что всё это можно получить и другими способами, например редиректом портов, vpn-ом и т.д. Но я для себя выбрал этот вариант, и мне он кажется самым удобным и надёжным.

Второе, что хотелось бы отмететь это опция:

```
X11Forwarding yes
```

Опять же по умолчанию отключена. Эта опция позволяет запускать X-приложения на удаленном компьютере с выводом изображения на локальный через ssh туннель. Требует хорошего канала связи, но внутри локальной сети вполне сносно работает. Особенностью является тот факт, что запустить можно, как отдельное приложение типа xcalc, так и целый DE, например, startkde. Соответсвенно, на запускаемой машине должен быть установлен X-сервер, что для unix-компьютеров нормально, но есть и реализация X-сервера для MS Windows.
Для запуска X-приложения через ssh используется опция **-X**, например команда:

```
user@localhost% ssh -X user@192.168.0.1 'oocalc'
```

запустит OpenOffice Calc на удаленной машине, а окно отрисует на локальной.

Последнее изменение: Mon Sep 22 23:20:56 2008

Автор: Dark

источник http://www.ounix.ru/index.php?page=article&id=19