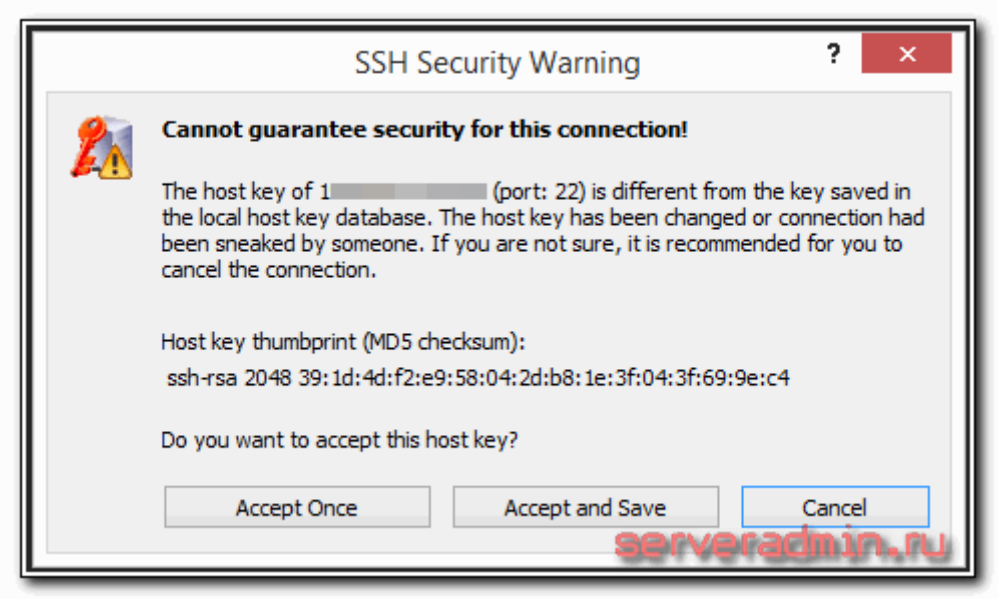
На днях столкнулся с необычной ситуацией, когда мне показалось, что кто-то хочет перехватить мой пароль от сервера, который я использую для подключения по ssh. На деле все оказалось намного проще. Никто не собирался уводить мой пароль. Но данная ситуация навела меня на мысль написать немного об этом.

Суть ситуации вот в чем. Я арендовал новый выделенный сервер у хостера с удаленной панелью управления и доступом к консоли сервера по ipmi. Установил чистую систему centos, настроил ее и подключился по ssh, используя ssh клиент на windows — **Xshell 5**.

При первом подключении по ssh к серверу, любой клиент выводит предупреждение о том, что отсутствует слепок rsa ключа сервера и предлагает его добавить.

Это нормальная ситуация, когда вы первый раз подключаетесь к серверу. Я начал настраивать сервер и в какой-то момент у меня сбрасывается соединение. Я отключаюсь от сервера. Пытаюсь подключиться снова и вижу предупреждение о том, что сохраненный слепок для этого сервера не соответствует тому, что сейчас предлагает сервер.



А вот это уже серьезно и я сразу напрягся. И всем советую не пропускать такие сообщения. Если это не первое ваше подключение по ssh, никаких изменений ключа быть не должно, если только вы его сами принудительно не изменили на сервере. Есть популярный вид атаки, когда где-то по пути вашего подключения вклинивается злоумышленник, сбрасывает ваше ssh подключение и запускает свой подменный сервер, которым ловит ваше новое

подключение. Признаком такого подменного сервера как раз и будет измененный отпечаток ключа. Если попытаетесь на нем авторизоваться, ваш логин с паролем утекут не туда, куда надо.

Первым делом я сразу же пошел на сервер через консоль и проверил публичный ключ, который использует ssh. Живет он по адресу */etc/ssh/ssh_host_rsa_key.pub*. Сравнил его с тем, что было сохранено у меня локально в Xshell 5 по адресу *C:\Users\user\Documents\NetSarang\SECSH\HostKeys*. Сами ключи совпадали. Я проверил отпечаток ключа, который отображает ssh клиент при подключении, с помощью команды:

```
# awk '{print $2}' /etc/ssh/ssh_host_rsa_key.pub | base64 -d | md5sum
39154df2e957042db8143f043f699ec4 -
```

Отпечаток не совпадал с тем, что мне предлагал ssh клиент при подключении. Стало очевидно, что я подключаюсь не к своему серверу. Авторизовываться не стал, пароль на сервере на всякий случай сменил. Стал думать, что делать. Сначала решил написать в тех поддержку. Но не был уверен, что кто-то серьезно ко всему этому отнесется, да и не понятно, где идет перехват. В дата центре или где-то у меня.

Решил просканить с помощью **nmap** свой внешний ip, по которому пытался подключиться. И тут все встало на свои места. Я насканил целую кучу открытых портов на сервере. Мне стало ясно, что это просто не мой сервер. Хостер мне выдал внешний ip, который уже используется на другом сервере. Отсюда все эти странности с разными сертификатами и обрывом соединений.

Написал о своих наблюдениях в тех поддержку. Мне подтвердили, что по ошибке выдали уже занятый ip адрес. В итоге дали новый, и я без проблем подключился к своему серверу. Такая неожиданная ситуация случилась, которая лишний раз напомнила о том, что не стоит расслабляться и соглашаться со всем, что выскакивает в окнах.

Не понравилась статья и хочешь научить меня администрировать? Пожалуйста, я люблю учиться. Комментарии в твоем распоряжении. Расскажи, как сделать правильно!

Помогла статья? Есть возможность отблагодарить автора