

Зертханалық сабақ №14: SSH қауіпсіздігін арттыру. Әр түрлі желілік ортадан қосылу.

SSH (Secure Shell) технологиясы қорғалған байланыс арқылы компьютерді қашықтықтан қауіпсіз басқаруға мүмкіндік береді. SSH Барлық жіберілген файлдарды, соның ішінде парольдерді шифрлайды, сонымен қатар кез-келген желілік протоколды жібереді. Құралдың дұрыс жұмыс істеуі үшін оны орнату ғана емес, сонымен қатар конфигурациялау қажет

Ubuntu-да SSH орнатыңыз

Егер сіз серверлік және клиенттік компьютерге орнатуды әлі аяқтамаған болсаңыз, онда алдымен соны жасауыңыз керек, өйткені бүкіл процедура өте қарапайым және көп уақытты қажет етпейді. Осы тақырып бойынша егжей-тегжейлі нұсқаулықпен келесі сілтемедегі басқа мақалада танысыңыз. Сондай-ақ, конфигурация файлын өңдеу және SSH жұмысын тексеру процедурасы көрсетілген, сондықтан бүгін біз басқа тапсырмаларға тоқталамыз.

RSA кілт жұбын құру

Жаңадан орнатылған SSH-де серверден клиентке және керісінше қосылуға арналған кілттер жоқ. Барлық осы параметрлер хаттаманың барлық компоненттерін қосқаннан кейін бірден қолмен орнатылуы керек. Кілт жұбы RSA алгоритмімен жұмыс істейді (rivest, Shamir және Adleman әзірлеушілерінің фамилияларының аббревиатурасы). Осы криптожүйенің арқасында Кілттерді шифрлау арнайы алгоритмдер арқылы жүзеге асырылады. Ашық кілттер жұбын жасау үшін консольге тиісті командаларды енгізіп, пайда болған нұсқауларды орындау керек.

1. "**Терминалмен**" кез-келген ыңғайлы әдіспен жұмыс істеуге өтіңіз, мысалы, оны мәзір немесе **Ctrl + Alt + T** пернелер тіркесімі арқылы ашыңыз



2. Ssh-keygen пәрменін енгізіп, **Enter** пернесін басыңыз.

```
patts@patts:~$ ssh-keygen
```

3. Кілттер сақталатын файл жасау сұралады. Егер сіз оларды әдепкі бойынша таңдалған жерде қалдырғыңыз келсе, **Enter** пернесін басыңыз

```
patts@patts:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/patts/.ssh/id_rsa):
```

4. Ашық кілтті кодтық сөйлеммен қорғауға болады. Егер сіз осы опцияны қолданғыңыз келсе, пайда болған жолға пароль жазыңыз. Енгізілген таңбалар көрсетілмейді. Кейін жаңа жолда оны қайталау қажет.

```
patts@patts:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/patts/.ssh/id_rsa): keys
Enter passphrase (empty for no passphrase):
```

5. Әрі қарай, сіз кілттің сақталғаны туралы хабарламаны көресіз, сонымен қатар оның кездейсоқ графикалық кескінімен таныса аласыз.

```
patts@patts:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/patts/.ssh/id_rsa): keys
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in keys.
Your public key has been saved in keys.pub.
The key fingerprint is:
SHA256:5Kc3jH2fND3H/TXhBMc80CZ750QqthxEGuyzuM0 patts@patts
The key's randomart image is:
+--[RSA 2048]-----+
|*.._BdBor          |
|o=ooX;oox         |
|==o = B..o        |
|++ o @ =          |
|o o * + S         |
|..o . .           |
|+ .               |
|. E               |
|                  |
+----[SHA256]-----+
patts@patts:~$
```

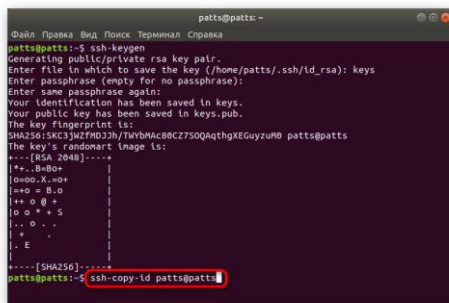
Енді жасалған кілттер жұбы бар — құпия және ашық, олар компьютерлер арасында әрі қарай қосылу үшін қолданылады. SSH аутентификациясы сәтті болуы үшін кілтті серверге қою керек.

Ашық кілтті серверге көшіру

Кілттерді көшірудің үш әдісі бар. Олардың әрқайсысы әртүрлі жағдайларда оңтайлы болады, мысалы, тәсілдердің бірі жұмыс істемейді немесе белгілі бір пайдаланушыға сәйкес келмейді. Біз ең қарапайым және тиімді нұсқадан бастап барлық үш нұсқаны қарастыруды ұсынамыз

1 нұсқа: ssh-copy-id командасы

Ssh-copy-id командасы амалдық жүйеге енгізілген, сондықтан оны орындау үшін қосымша компоненттерді орнатудың қажеті жоқ. Кілтті көшіру үшін қарапайым синтаксисті сақтаңыз. "**Терминалда**" ssh-copy-id `username@remote_host` енгізу керек, мұнда `username@remote_host` — қашықтағы компьютердің атауы.



```
patts@patts:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/patts/.ssh/id_rsa): keys
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in keys.
Your public key has been saved in keys.pub.
The key fingerprint is:
SHA256:5Kc3jz7fMD3h/TvYbMAC8CZ750QaqtgXEGuyzuM0 patts@patts
The key's randomart image is:
+--[RSA 2048]-----+
|+..B=Bo+          |
|o=oo.X..oo+      |
|+..o = B.o        |
|+..o @ +          |
|o o * + S         |
|..o . .           |
|..+               |
|.E                |
|                  |
+---[SHA256]-----+
patts@patts:~$ ssh-copy-id patts@patts
```

Бірінші қосылу кезінде сіз мәтінмен хабарлама аласыз:

```
The authenticity of host '203.0.113.1 (203.0.113.1)' can't be established.
ECDSA key fingerprint is fd:fd:d4:f9:77:fe:73:84:e1:55:00:ad:d6:6d:22:fe.
Are you sure you want to continue connecting (yes/no)? yes
```

Қосылымды жалғастыру үшін **yes** нұсқасын көрсету керек. Осыдан кейін қызметтік бағдарлама `id_rsa` файлы түрінде кілт іздейді. бұрын құрылған **pub**. Сәтті табылғаннан кейін келесі нәтиже көрсетіледі:

```
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any
that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now
it is to install the new keys
username@203.0.113.1's password:
```

Утилитаның оған кіруі үшін қашықтағы хосттың паролін көрсетіңіз. Құрал деректерді жалпыға ортақ кілт файлынан көшіреді `~/.ssh/id_rsa.pub`, содан кейін экранда хабарлама пайда болады:

```
Number of key(s) added: 1
```

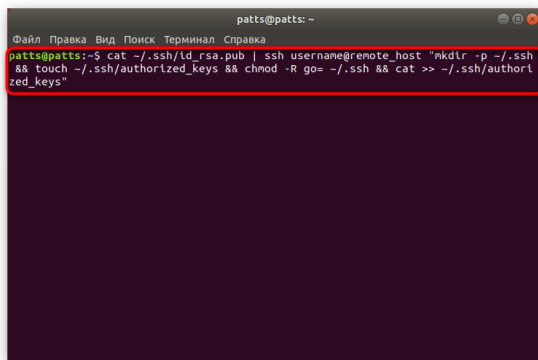
Now try logging into the machine, with: "ssh 'username@203.0.113.1'" and check to make sure that only the key(s) you wanted were added.

Мұндай мәтіннің пайда болуы кілт қашықтағы компьютерге сәтті жүктелгенін білдіреді, енді қосылуда ешқандай проблемалар болмайды.

2 нұсқа: SSH арқылы ашық кілтті көшіру

Егер сіз жоғарыда аталған қызметтік бағдарламаны пайдалана алмасаңыз, бірақ қашықтағы **SSH** серверіне кіру үшін пароль болса, пайдаланушы кілтін қолмен жүктей аласыз, осылайша қосылған кезде одан әрі тұрақты аутентификацияны қамтамасыз ете аласыз. Бұл үшін **cat** пәрмені қолданылады, ол файлдағы деректерді оқиды, содан кейін олар серверге жіберіледі. Содан соң Консольге жолды енгізу қажет

```
cat ~/.ssh/id_rsa.pub | ssh username@remote_host "mkdir -p ~/.ssh && touch  
~/.ssh/authorized_keys && chmod -R go= ~/.ssh && cat >> ~/.ssh/authorized_keys".
```



Хабарлама пайда болған кезде

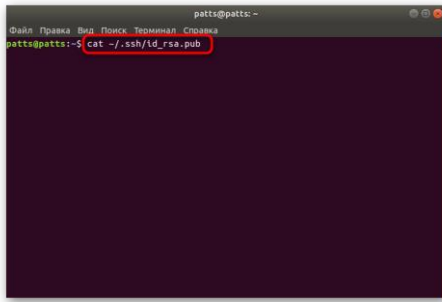
```
The authenticity of host '203.0.113.1 (203.0.113.1)' can't be established.  
ECDSA key fingerprint is fd:fd:d4:f9:77:fe:73:84:e1:55:00:ad:d6:6d:22:fe.  
Are you sure you want to continue connecting (yes/no)? yes
```

қосылуды жалғастырыңыз және серверге кіру үшін құпия сөзді енгізіңіз.

Осыдан кейін ашық кілт автоматты түрде **authorized_keys** конфигурация файлының соңына көшіріледі.

3 нұсқа: ашық кілтті қолмен көшіру

Қашықтағы компьютерге SSH сервері арқылы кіру мүмкіндігі болмаған жағдайда, жоғарыда сипатталған барлық әрекеттер қолмен орындалады. Мұны істеу үшін алдымен **cat** ~/пәрмені арқылы серверлік компьютердегі кілт туралы ақпаратты біліңіз.ssh/id_rsa.pub.

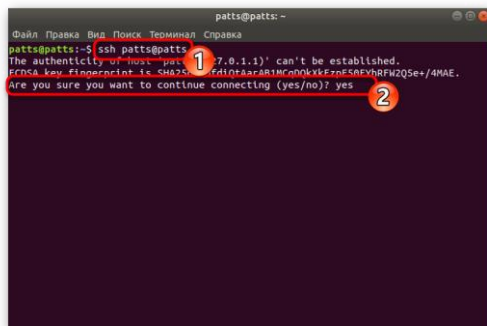


Экранда келесі жол пайда болады: ssh-rsa + таңбалар жиынтығы түріндегі кілт== demo@test. Осыдан кейін қашықтағы құрылғыға жұмысқа өтіңіз, онда mkdir-p ~/арқылы жаңа каталог жасаңыз.ssh. Ол қосымша authorized_keys файлын жасайды. Әрі қарай, echo + қоғамдық кілт жолы > > ~/арқылы бұрын білген кілтті салыңыз.ssh/authorized_keys. Осыдан кейін сіз парольдерді пайдаланбай сервермен аутентификацияны қолдана аласыз.

Жасалған кілт арқылы сервердегі Аутентификация

Алдыңғы бөлімде сіз қашықтағы компьютердің кілтін серверге көшірудің үш әдісі туралы білдіңіз.

Мұндай әрекеттер парольді пайдаланбай қосылуға мүмкіндік береді. Бұл процедура ssh ssh **username@remote_host** енгізу пәрмені арқылы орындалады, мұнда username@remote_host - қалаған компьютердің пайдаланушы аты және хосты. Бірінші қосылымда сізге бейтаныс байланыс туралы хабарланады және **yes** опциясын таңдау арқылы жалғастыра аласыз.



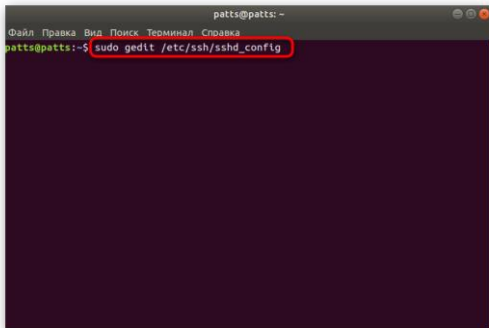
Егер кілт жұбын құру кезінде кілт сөз тіркесі (*passphrase*) орнатылмаған болса, қосылым автоматты түрде пайда болады. Әйтпесе, **SSH**-мен жұмыс істеуді жалғастыру үшін алдымен оны енгізу керек.

Пароль арқылы аутентификацияны өшіру

Кілттерді көшіруді сәтті орнату серверге парольді пайдаланбай кіруге болатын жағдайда қарастырылады. Алайда, осылайша аутентификация мүмкіндігі

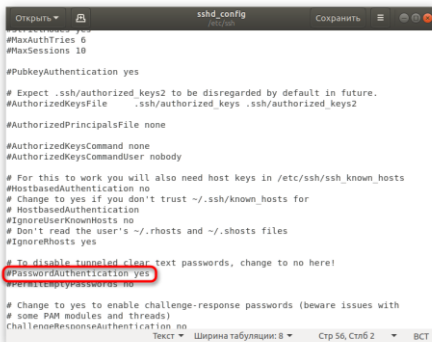
зиянкестерге парольді таңдауға және қорғалған қосылымды бұзуға арналған құралдарды пайдалануға мүмкіндік береді. Мұндай жағдайлардан өзіңізді қорғау **SSH** конфигурация файлындағы құпия сөзді толығымен өшіруге мүмкіндік береді. Бұл үшін қажет:

1. "Терминалда" **sudo gedit /etc/ssh/sshd_config** пәрменін пайдаланып редактор арқылы конфигурация файлын ашыңыз.



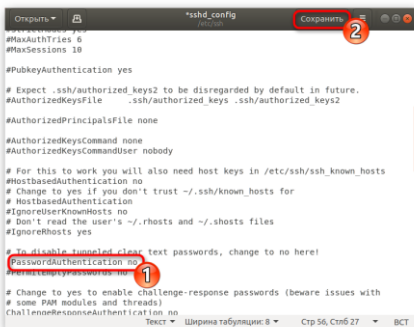
```
pattt@pattt:~$ sudo gedit /etc/ssh/sshd_config
```

2. "PasswordAuthentication" жолын тауып, параметрге түсініктеме беру үшін # белгісін алып тастаңыз.



```
#PasswordAuthentication yes
```

3. Мәнді **no** етіп өзгертіңіз және ағымдағы конфигурацияны сақтаңыз.



```
#PasswordAuthentication no
```

4. Редакторды жауып, **sudo systemctl restart ssh** серверін қайта іске қосыңыз.

```
pattis@pattis:~$ sudo gedit /etc/ssh/sshd_config
[sudo] password for pattis:
** (gedit:3884): WARNING **: 21:48:29.261: Set document metadata failed: украинська мовна метадані:gedit-spell language не підтримується
** (gedit:3884): WARNING **: 21:48:29.261: Set document metadata failed: украинська мовна метадані:gedit-encoding не підтримується
** (gedit:3884): WARNING **: 21:48:29.261: Set document metadata failed: украинська мовна метадані:gedit-position не підтримується
pattis@pattis:~$ sudo systemctl restart ssh
```

Пароль аутентифікація ошіреледі және серверге тек RSA алгоритмі бар арнайы жасалған кілттерді қолдана отырып кіруге болады.

Стандартты firewall орнату

Ubuntu-да желіні қорғау әдепкі бойынша брандмауэр болып табылады Uncomplicated Firewall (UFW). Ол шешуге мүмкіндік береді қосылыстар үшін сайланған сервистердің. Әрбір бағдарлама осы құралда өз профилін жасайды, ал UFW оларды қосылуға рұқсат беру немесе тыйым салу арқылы басқарады. SSH профилін тізімге қосу арқылы орнату келесідей:

1. Sudo ufw app list пәрмені арқылы firewall профильдерінің тізімін ашыңыз.

```
pattis@pattis:~$ sudo ufw app list
```

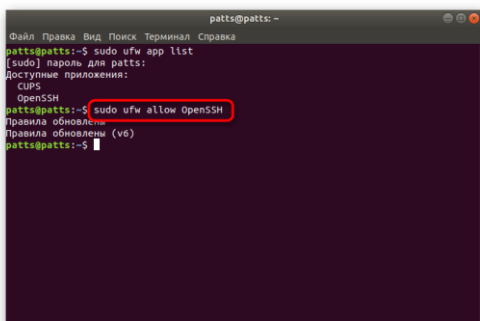
2. Ақпаратты көрсету үшін есептік жазбаның құпия сөзін енгізіңіз

```
pattis@pattis:~$ sudo ufw app list
[sudo] password for pattis:
```

3. Сіз қол жетімді қосымшалардың тізімін көресіз, олардың арасында OpenSSH болуы керек.

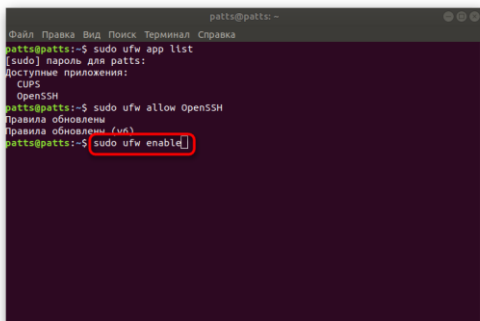
```
pattis@pattis:~$ sudo ufw app list
[sudo] password for pattis:
UFW status: inactive
UFW default: deny (incoming), allow (outgoing), disabled (reset)
UFW allowed:
  OpenSSH
```

4. Енді SSH арқылы қосылыстарға рұқсат беру керек. Мұны істеу үшін оны sudo ufw allow OpenSSH көмегімен рұқсат етілген профильдер тізіміне қосыңыз.



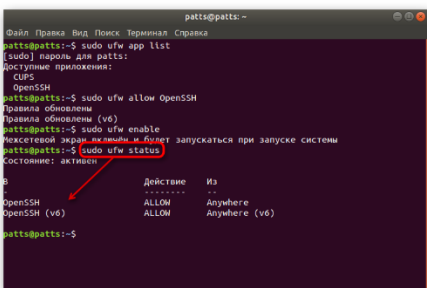
```
patts@patts:~$ sudo ufw app list
[sudo] пароль для patts:
Доступные приложения:
  CUPS
  OpenSSH
patts@patts:~$ sudo ufw allow OpenSSH
Правила обновлены
Правила обновлены (v6)
patts@patts:~$
```

5. Ережелерді жаңарту арқылы firewall-ды қосыңыз, sudo ufw enable



```
patts@patts:~$ sudo ufw app list
[sudo] пароль для patts:
Доступные приложения:
  CUPS
  OpenSSH
patts@patts:~$ sudo ufw allow OpenSSH
Правила обновлены
Правила обновлены (v6)
patts@patts:~$ sudo ufw enable
Последней эрдің ақпараты бойынша, біліңіз: запускується при запуску системи
patts@patts:~$
```

6. Қосылымдардың рұқсат етілгеніне сену үшін sudo ufw status бағдарламасын жазып алу керек, содан кейін сіз желінің күйін көресіз



```
patts@patts:~$ sudo ufw status
Состояние: активен

```

	Действие	Из
OpenSSH	ALLOW	Anywhere
OpenSSH (v6)	ALLOW	Anywhere (v6)

```
patts@patts:~$
```

Бұл жерде Ubuntu-да SSH конфигурациясы туралы нұсқаулар аяқталды. Конфигурация файлының және басқа параметрлердің одан әрі параметрлерін әр пайдаланушы өз сұрауларына сәйкес жүзеге асырады. Сіз SSH-тің барлық компоненттерінің әрекетімен хаттаманың ресми құжаттамасында таныса аласыз.