Getting started with SSH Keys with a free SYN Shop VM Host

mrjones

SYN Shop
Wednesday May 16, 2018

mrjones@plip.com
plip.com/sshkeys

v5.0

Agenda

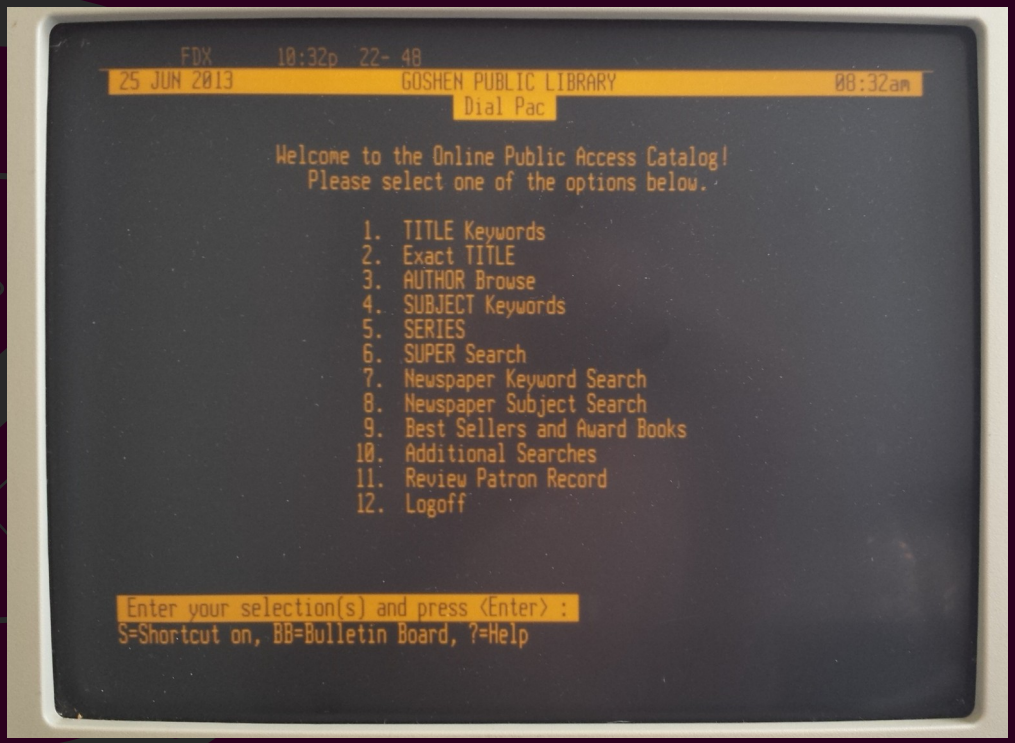
- Tech Review (Tech Review)
- How to Generate (Keys)
- Keys: Installing and using on free VM (Use)

Follow along at: plip.com/sshkeys

TECH REVIEW

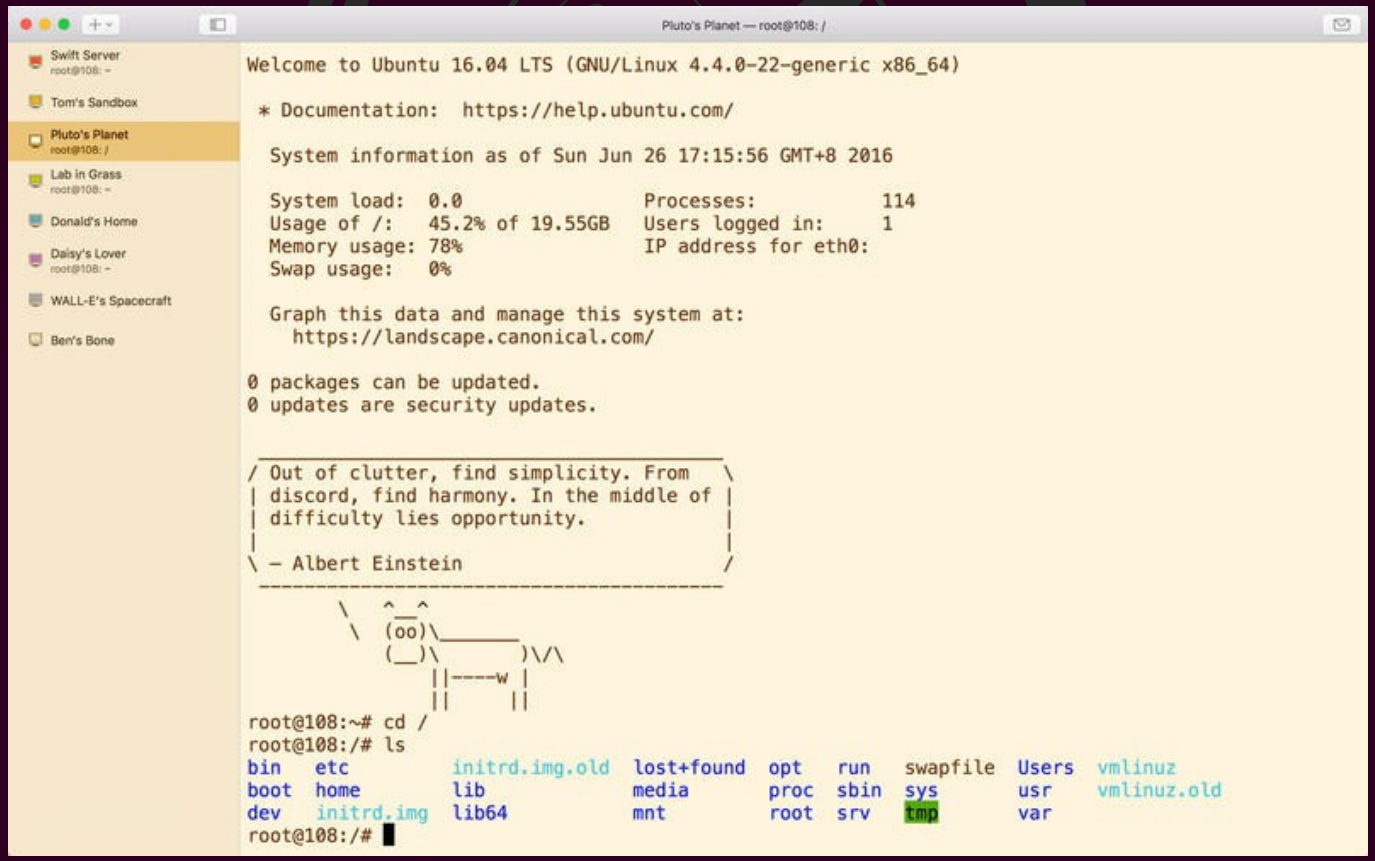
Tech Review: Before & After

- Telnet - remember telnet? Unencrypted
- Telnet First developed in 1969
- SSH v1.0 1995
- SSH v2.0 2006



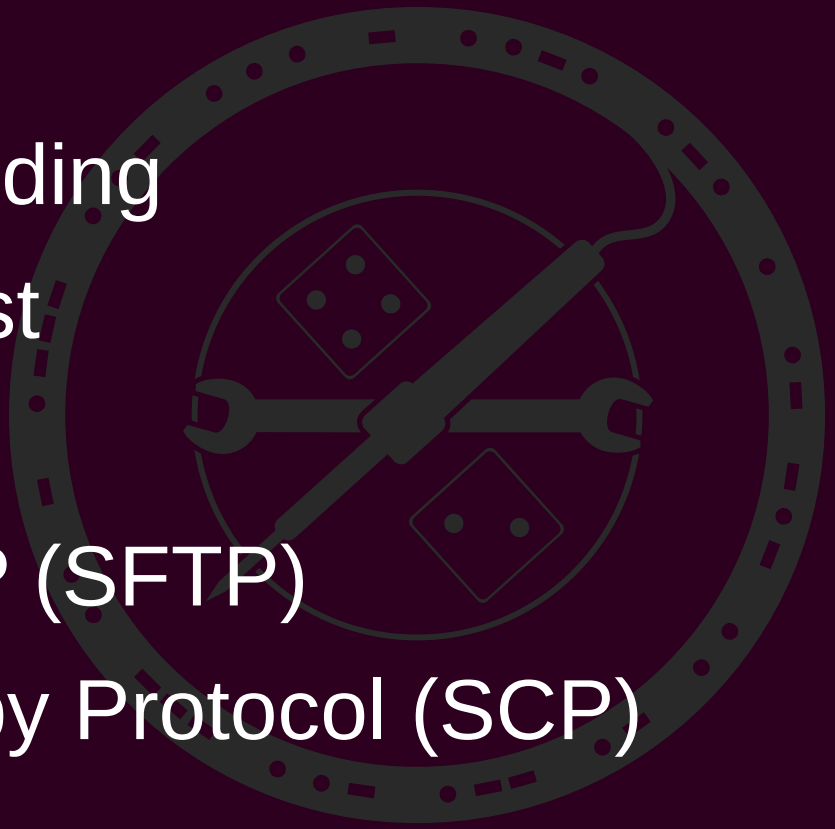
Tech Review: SSH More better

- Telnet, but Encrypted by default!
- Stands for ***S***ecure ***Sh***ell



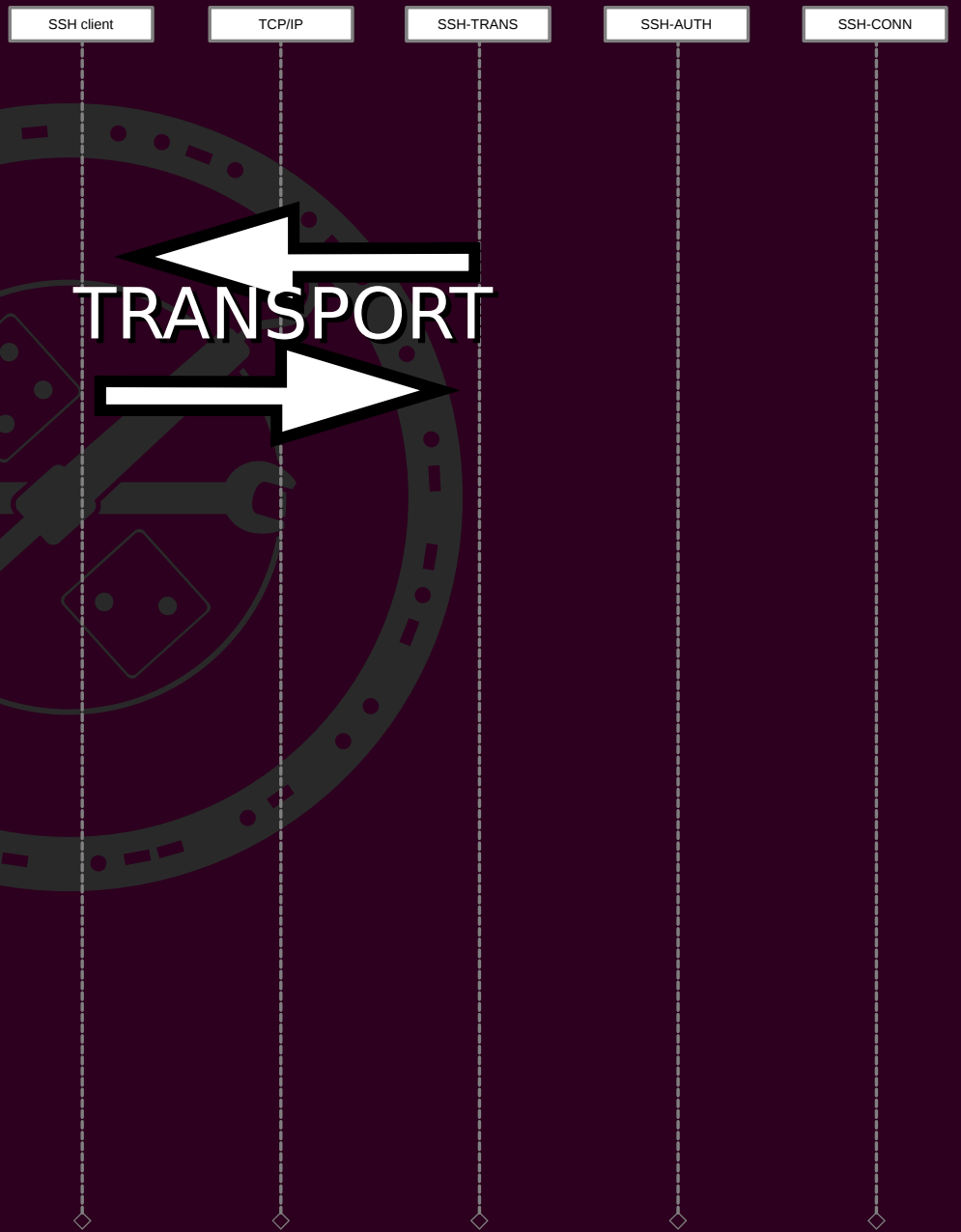
Tech Review: Features & Uses

- Shell
- Port Forwarding
- Bastion Host
- SSH Agent
- Secure FTP (SFTP)
- Secure Copy Protocol (SCP)



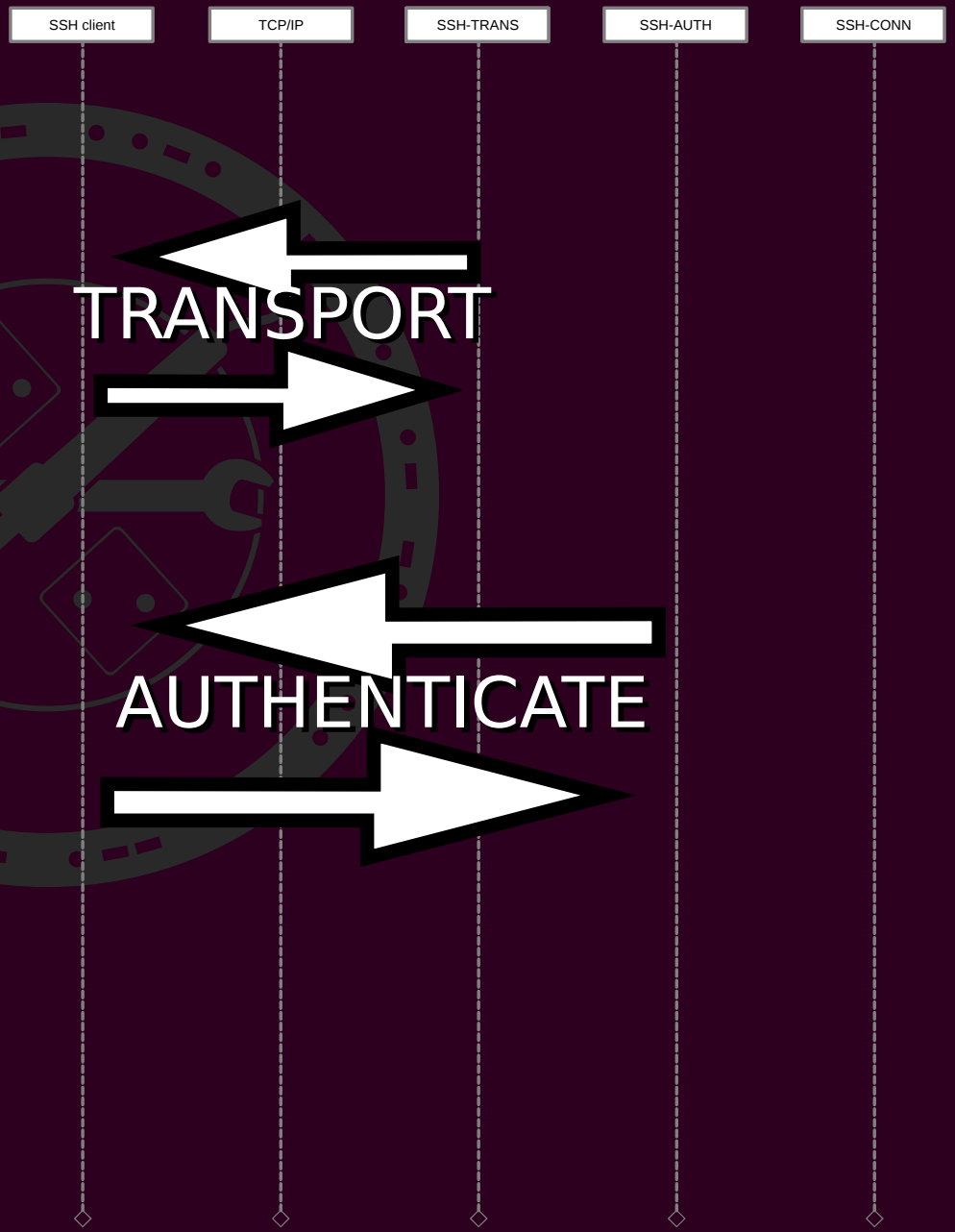
Tech Review: SSH Connections

1. Transport layer - Secure channel via TCP. Symmetric encryption via Diffie-Hellman



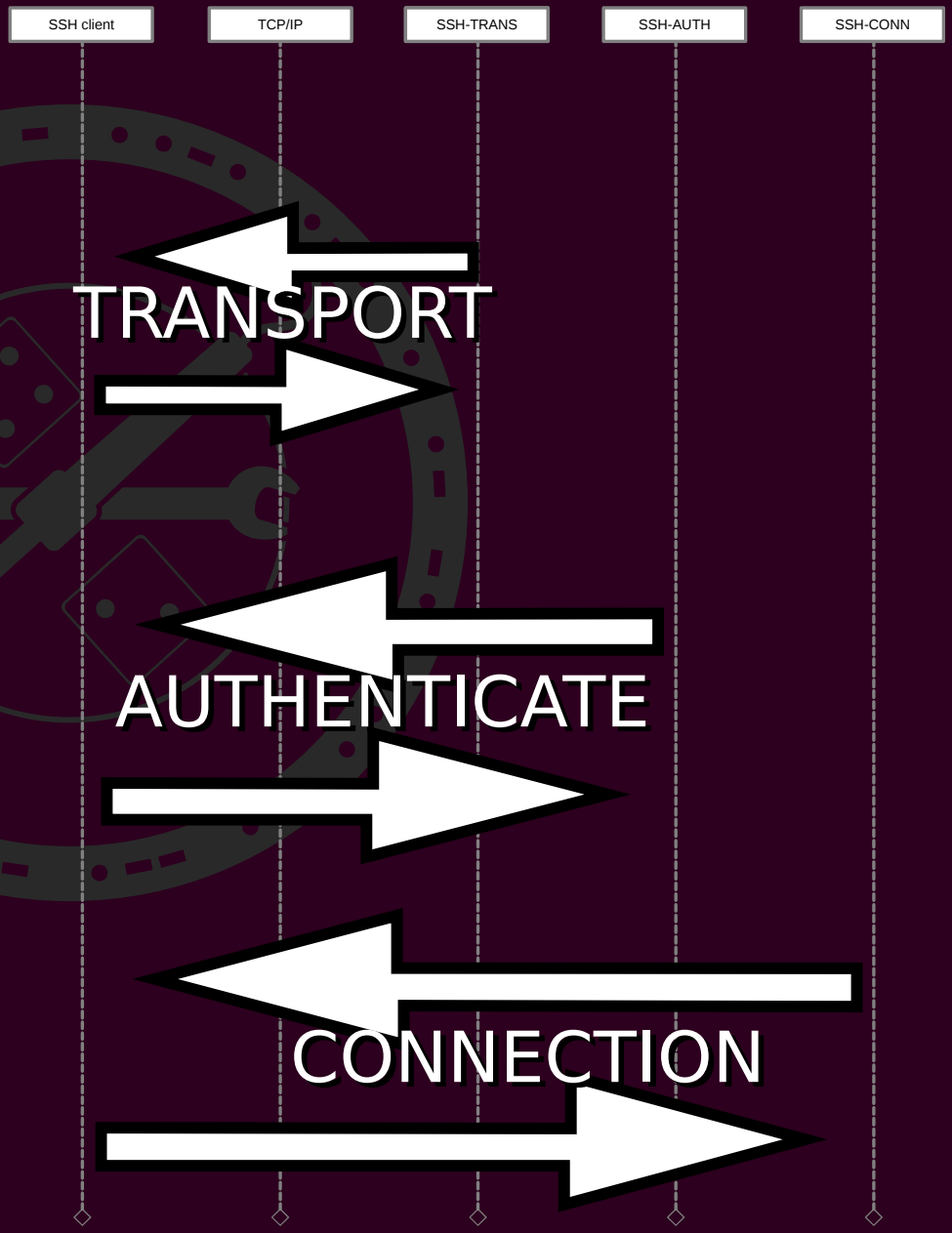
Tech Review: SSH Connections

2. Authentication layer - Verify user via password or SSH key



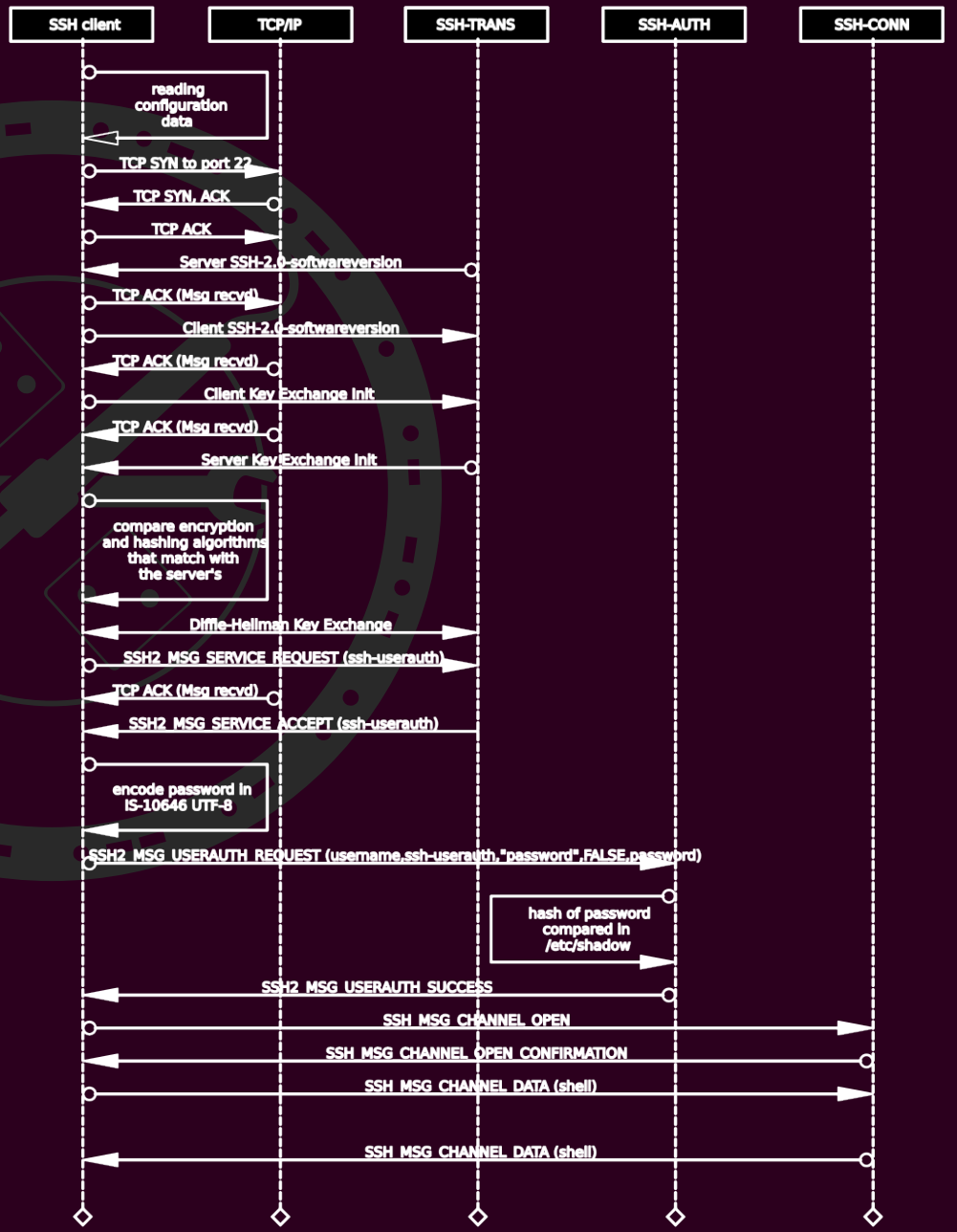
Tech Review: SSH Connections

3. Connection Layer
   - Shell can be used



Tech Review: SSH Connections

1. Transport layer
2. Authentication layer
3. Connection Layer



Tech Review: Authentication

- Password (boo!) - hash against /etc/shadow
- SSH Keys (yay!) - aka asymmetric encryption aka public key encryption
- Others (keyboard-interactive, GSSAPI)

Tech Review: SSH Keys

- `ssh-keygen` generates a key pair of keys public & private
- private key is ***never*** shared
- upload public key to the server
- server encrypts secret message with public key
- client proves (authenticates) itself by decrypting the message with the private key

Tech Review: SSH files

- .ssh
- .ssh/config
- .ssh/id_rsa
- .ssh/id_rsa.pub
- .ssh/id_ed25519
- .ssh/id_ed25519.pub
- .ssh/known_hosts
- .ssh/authorized_keys

Tech Review: SSH files

- .ssh
- .ssh/config
- .ssh/id_rsa
- .ssh/id_rsa.pub
- .ssh/id_ed25519
- .ssh/id_ed25519.pub
- .ssh/known_hosts
- .ssh/authorized_keys

Parent directory of all ssh files. Likely hidden in directory listings. “`cd;ls -ahl .ssh/`” to see it’s contents

Tech Review: SSH files

- .ssh
- .ssh/config
- .ssh/id_rsa
- .ssh/id_rsa.pub
- .ssh/id_ed25519
- .ssh/id_ed25519.pub
- .ssh/known_hosts
- .ssh/authorized_keys

Config file for all SSH connections. Handy to specify host specific or global settings. Remote port, alias for long hostname, path to private key, specific users and...Bastion Hosts!

Tech Review: SSH files

- .ssh
- .ssh/config
- .ssh/id_rsa
- .ssh/id_rsa.pub
- .ssh/id_ed25519
- .ssh/id_ed25519.pub
- .ssh/known_hosts
- .ssh/authorized_keys

RSA Private key – DO NOT SHARE! KEEP SAFE!

Tech Review: SSH files

- .ssh
- .ssh/config
- .ssh/id_rsa
- .ssh/id_rsa.pub ← RSA Public key – Safe to send anywhere!
- .ssh/id_ed25519
- .ssh/id_ed25519.pub
- .ssh/known_hosts
- .ssh/authorized_keys

Tech Review: SSH files

- .ssh
- .ssh/config
- .ssh/id_rsa
- .ssh/id_rsa.pub
- .ssh/id_ed25519 ⟵ ed25519 Private key – DO NOT SHARE! KEEP SAFE!
- .ssh/id_ed25519.pub
- .ssh/known_hosts
- .ssh/authorized_keys

Tech Review: SSH files

- .ssh
- .ssh/config
- .ssh/id_rsa
- .ssh/id_rsa.pub
- .ssh/id_ed25519
- .ssh/id_ed25519.pub
- .ssh/known_hosts
- .ssh/authorized_keys

← ed25519 Public key – Safe to send anywhere!

Tech Review: SSH files

- .ssh
- .ssh/config
- .ssh/id_rsa
- .ssh/id_rsa.pub
- .ssh/id_ed25519
- .ssh/id_ed25519.pub
- .ssh/known_hosts ←
- .ssh/authorized_keys

Gathers servers you have connected to in the past. Will grow in size as you connect to more and more servers. Captures finger print upon first connection to server

Tech Review: SSH files

- .ssh
- .ssh/config
- .ssh/id_rsa
- .ssh/id_rsa.pub
- .ssh/id_ed25519
- .ssh/id_ed25519.pub
- .ssh/known_hosts
- .ssh/authorized_keys ← Put any public keys you want to authorize to connect to this server here. (not used on client machine)


KEYS

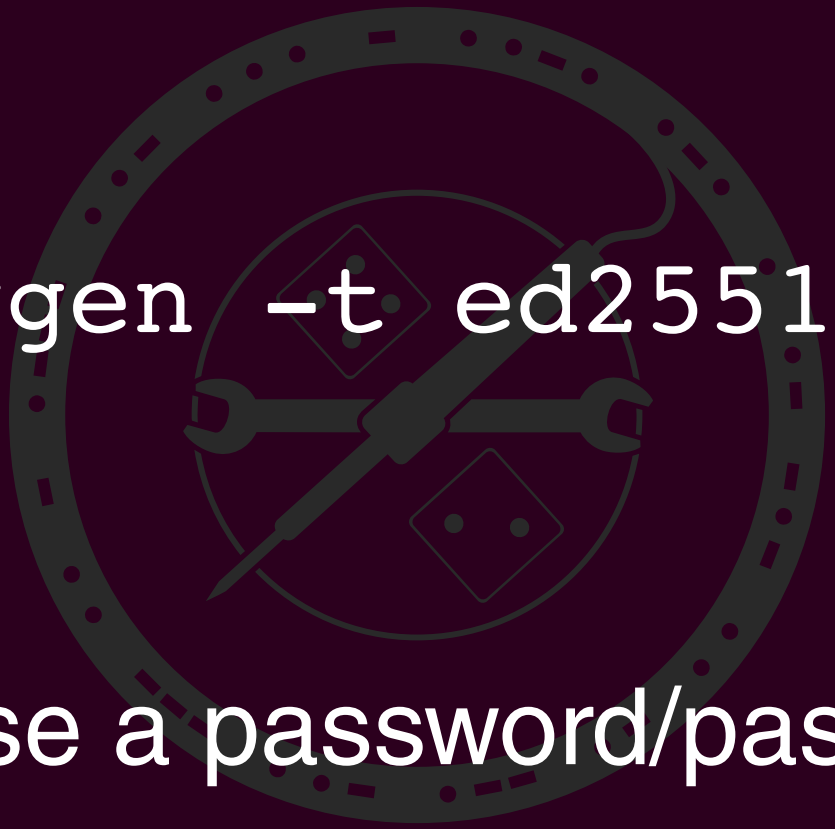
Keys: ed25519 type

```
cat /tmp/deleteme

-----BEGIN OPENSSH PRIVATE KEY-----

B3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACCNSQA33K+EGj5HbswDVyTHqnomHBL/XgVYPhDdAor0EwAAAJi3fsk0t37J
NAAAAAtzc2gtZWQyNTUxOQAAACCNSQA33K+EGj5HbswDVyTHqnomHBL/XgVYPhDdAor0E
AAAEAA957sXvHPYfUTczho/7TCY3Xppau36YbqoBEJ1JFVg41JADfcr4QaPkduzANXJMeq
eiYcEv9eBVg+EN0CivQTAAAAEG1yam9uZXNAYWlyYnVudHUBAgMEBQ==

-----END OPENSSH PRIVATE KEY-----

cat /tmp/deleteme.pub

ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAII1JADfcr4QaPkduzANXJMeqeiYcEv9eBVg+EN0CivQT
mrjones@airbuntu
```

Keys: rsa type

```
cat /tmp/deleteme

-----BEGIN RSA PRIVATE KEY-----

MIIJKAIBAAKCAgEAwUlgeHfMOBiMaLZCU5AngG4Mg/l0ewE0DrKBFlAmy3W0LeWq
WKG+ZzVOqyJX8GWs0QLzaMlLZBrURTb4EXAOdzvGmMUmoP1GKQ4BanpKaEEStKe1
iuokdqH97hFBc7fpBp6bB179FG0705IOGfgCmMMhMgTyNmX7RRokUwAEDvEaS8rI
01xxfiqOEapce7c8c1Z4HPpqNZhYK1zfbEQKDB9salAlHj5qcljtScHFSEG3Q7vD
ZLj6Kq1DobASfL/6f5vEn+PBCvSRw2hQE12VfX16P7pn2l0xd+Sd4wz4ZflswX2b
fjc/tLZXAknsiiznITZf41kNJ1j1/QB6dXhdhVs16BxYktS9fpY4sPbNmx31E/0I
1hCdwm76qqPPGWnpUajKubpeiafGaw3p2CJBAOyqmpiU6x6OV+B54LZDysjHvwbB
+3mDsjvScQE36flg9vdRk4QH/Seg+ZFqhLhc/04vT9gGCLrLiSP1L3rhd1cEpMVc
mA+XhMnnBF1BpSWZFK2CWTHkdidts3QEjNVxjjZ0X6nO4u0B83PplXpUvdmoPCuU
btMpXnmzuENhUZjJWXex2ESzVcAfJTn8cr9ecVJQQnEfwkCPCddSwBuXS/0tTXcD
0yCrKcrvmBRrMb+AlmL76BDPNcgX8GE5A4/8QoEfVRmNUIFHHNX8rrOjCncCAwEA
AQKCAgAHtlzSEb2lU11u5C7bVLouxrVbIr4CFnc0Su0ZrdMOdUDeP/a/GJ0XUyoz
a+hkYDo4EM0TlkyazvM/W8UkNPtuyITRHbS/4btF8hgeXojPhiEv8i0tQNB5p1cR
g8C/1EvJBtUawzCH+x/S/lXvtVStMcQGUeo0P3d6N2PRqAOBcR9ifNHslRi2Nw56
J/kOuq3/0Ch0x40rXEvQVyFXGZPpDevuhgolHcpzi5bURZYQnwan/jr6ruLUhxtW
vUbPkX12UAnVc2oFfOLAEE55p1dKrZIOLurr7KIHraibIa5bq0sqoU9uBthU5p2s
KrT0gnwqeBf1Y11B/6u5D6bTPx1EHgz7LX5zL93inAPLRyl8tdXizXXisL1Ec1vm
Ha5bXVnUYWZmrgOosgjOcscxXOeOwE63cxWOhpuN9G3kuXLugZrWnKzFPZX+/zM5
0+pD4QKCAQA4O2Ojmb+vyFfgl5PG/Z3btBQFfIfq7QFsArsCx+4jflxFMoe3gWaa
37Ls7RZALskN3ILyosm4oWNORrg8kbi9Q6eNifEw0lDbOWZeslbgwJWNhN6/EIL2
PGQSXagjyVsk0MaD0T2GKfBsFbSN9Xlq8MNjN2/oHVowZu5qaRmrjpgkxph0MTO2
UcwVLrzVc5iXFcAGjGGc1GCsfRoNo5iZo/o4KIW0m3BTQzr/Q+DJmIEiLCN3hQYM
SPG9rekR4jyfGeq1MlM+Zfd5g1s+6Pg6v4qKUzW7KWlGiJvHglEvRXG12g41XZIp
qMn/EmQ2aU+H/C+tb5yIayYy7qWHu8z/AoIBACsySgzfXGWy4Pxyw34IHhLdQ3O5
JEMwx3wSxl5lnUk4oGLAo2fjFqfbMMwFFXbIni7mxaKU3wjTHQSBKDEZoUQXYx5s
WCs3B2anPNnRZ/V7Gty/fJaVsdlyW8n3+b67MvtkjpR7PwIkIcqY9nBTMvWmJM73
94Y1WW6xB2V6trAJMxVYnTWbqmYZZI76L6GOBTWZmOQlgVKysfuc5fNgz4h/9sQv
AD7HNvas1Fi6TgDAH4E91osDnhIXKq/+fIKqxVxXlydruY018+Bzoj803HD4BkW0
z2sHtxywGGN5rIfPzOA5r3cmWxdPFhe0JmR2cyug8H8NKw1Z9ZCkVdaszw=

-----END RSA PRIVATE KEY-----

➜  ~ cat /tmp/deleteme.pub

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDBSWB4d8w4GIxotkJTkCeAbgyD+XR7ATQOsoEWUCbLdbQt5apYob5nN
U6rIlfwZazRAvNoyUtkGtRFNvgRcA53O8aYxSag/UYpDgFqekpoQRK0p7WK6iR2of3uEUFzt+kGnpsHXv0UbTvTkg4Z+
AKYwyEyBPI2ZftFGiRTAAQO8RpLysjTXHF+Ko4Rqlx7tzxzVngc+mo1mFgrXN9sRAoMH2xqUCUePmpyWO1JwcVIQbdDu
8NkuPoqrUOhsBJ8v/p/m8Sf48EK9JHDaFATXZV9fXo/umfaXTF35J3jDPhl+WzBfZt+Nz+0tlcCSeyKLOchNl/jWQ0nW
PX9AHp1eF2FWzXoHFiS1L1+ljiw9s2bHfUT/QjWEJ3Cbvqqo88ZaelRqMq5ul6Jp8ZrDenYIkEA7KqamJTrHo5X4Hngt
kPKyMe/BsH7eYOyO9JxATfp+WD291GThAf9J6D5kWqEuFz/Ti9P2AYIusuJI/UveuF3VwSkxVyYD5eEyecEXUGlJZkUrY
JZMeR2J22zdASM1XGONnRfqc7i7QHzc+mVelS92ag8K5Ru0yleebO4Q2FRmMlZd7HYRLNVwB8lOfxyv15xUlBCcR/CQI8J1
1LAG5dL/S1NdwPTIKspyu+YFGsxv4CWYvvoEM81yBfwYTkDj/xCgR9VGY1QgUcc1fyus6MKdw== mrjones@airbuntu
```

Keys: Generate on MacOS/Linux



```
ssh-keygen -t ed25519
```

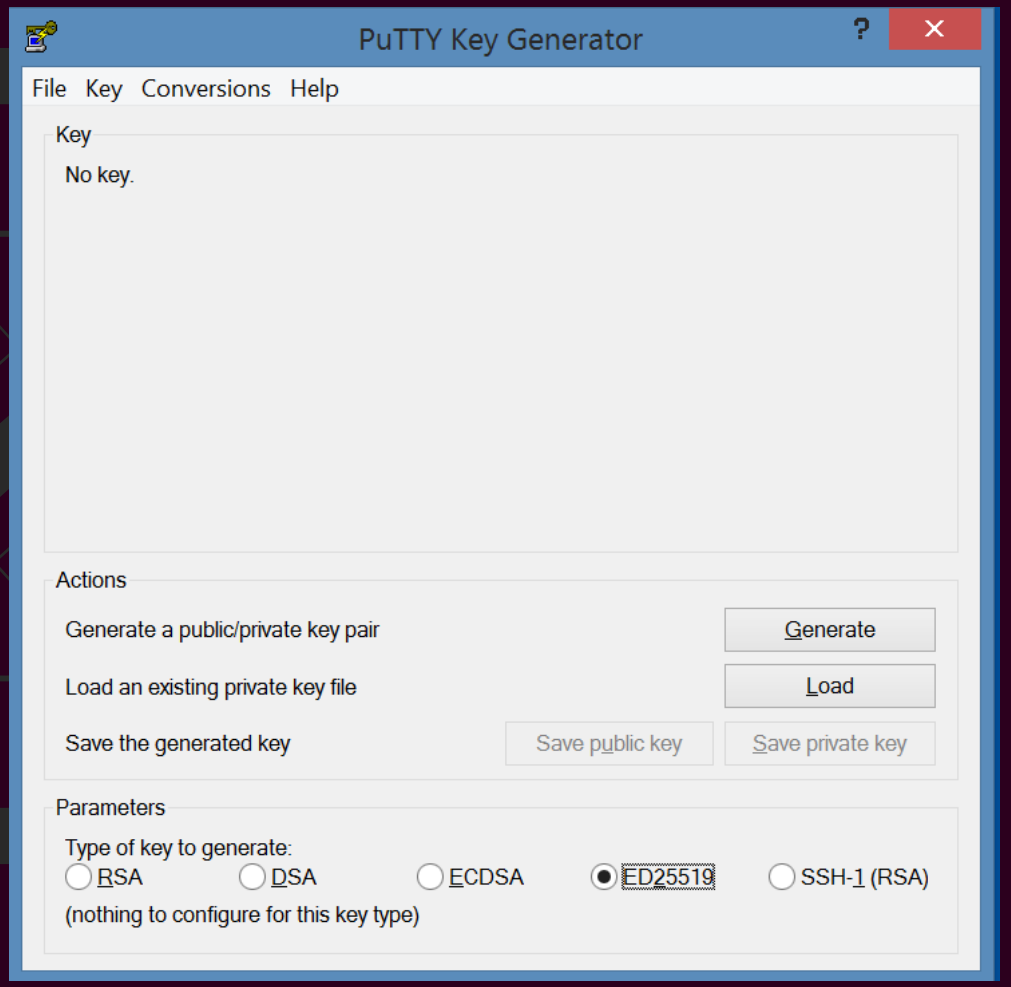
Please use a password/passphrase!

Keys: Generate on MacOS/Linux

```
ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /tmp/deleteme.
Your public key has been saved in /tmp/deleteme.pub.
The key fingerprint is:
SHA256:nvGfnBEyakw4VvfnBpR9HDgk/iQ mrjones@airbuntu
The key's randomart image is:
+--[ED25519 256]--+
|          ....   |
|         . .o .  |
|          Eo.o . |
|       o oo^o=   |
|        ++*=@    |
+----[SHA256]-----+
```

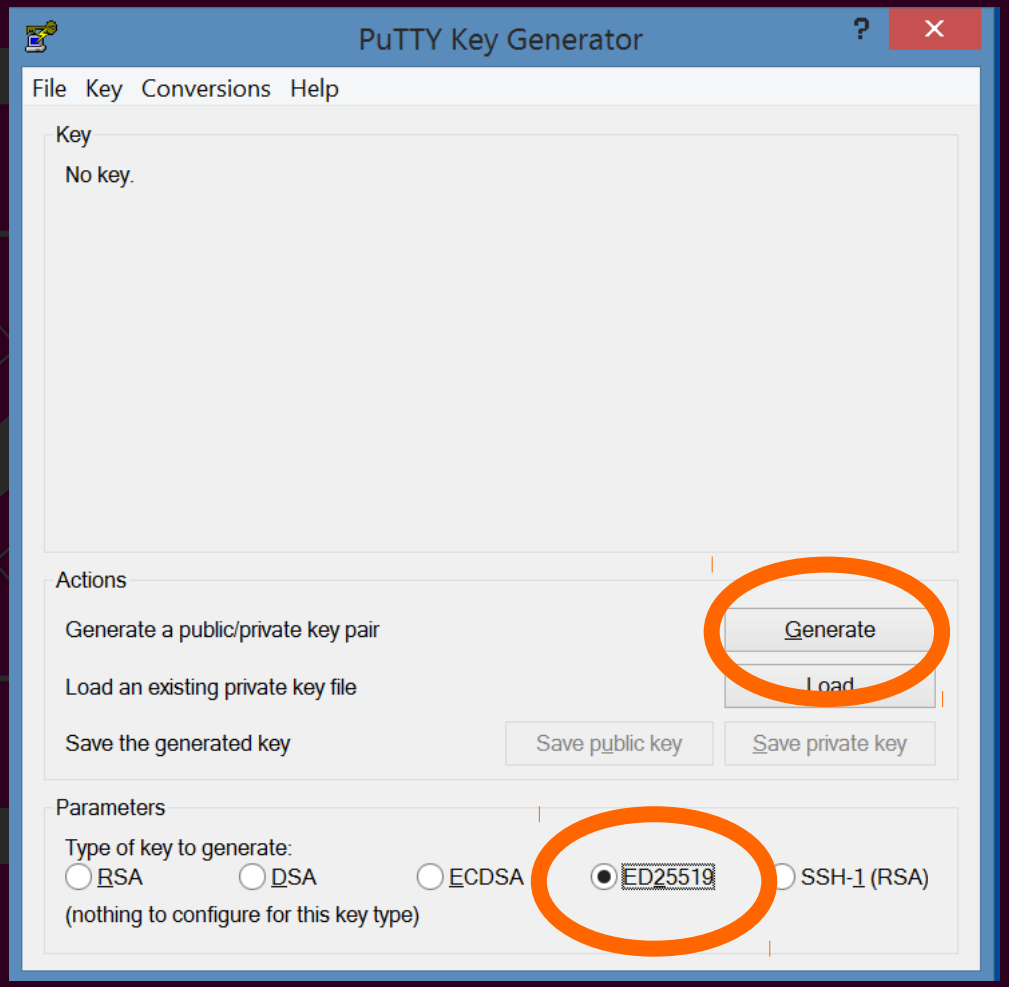
Keys: Generate on Windows

- Install Putty (chiark.greenend.org.uk)
- Start menu → All Programs → PuTTY → PuTTYgen



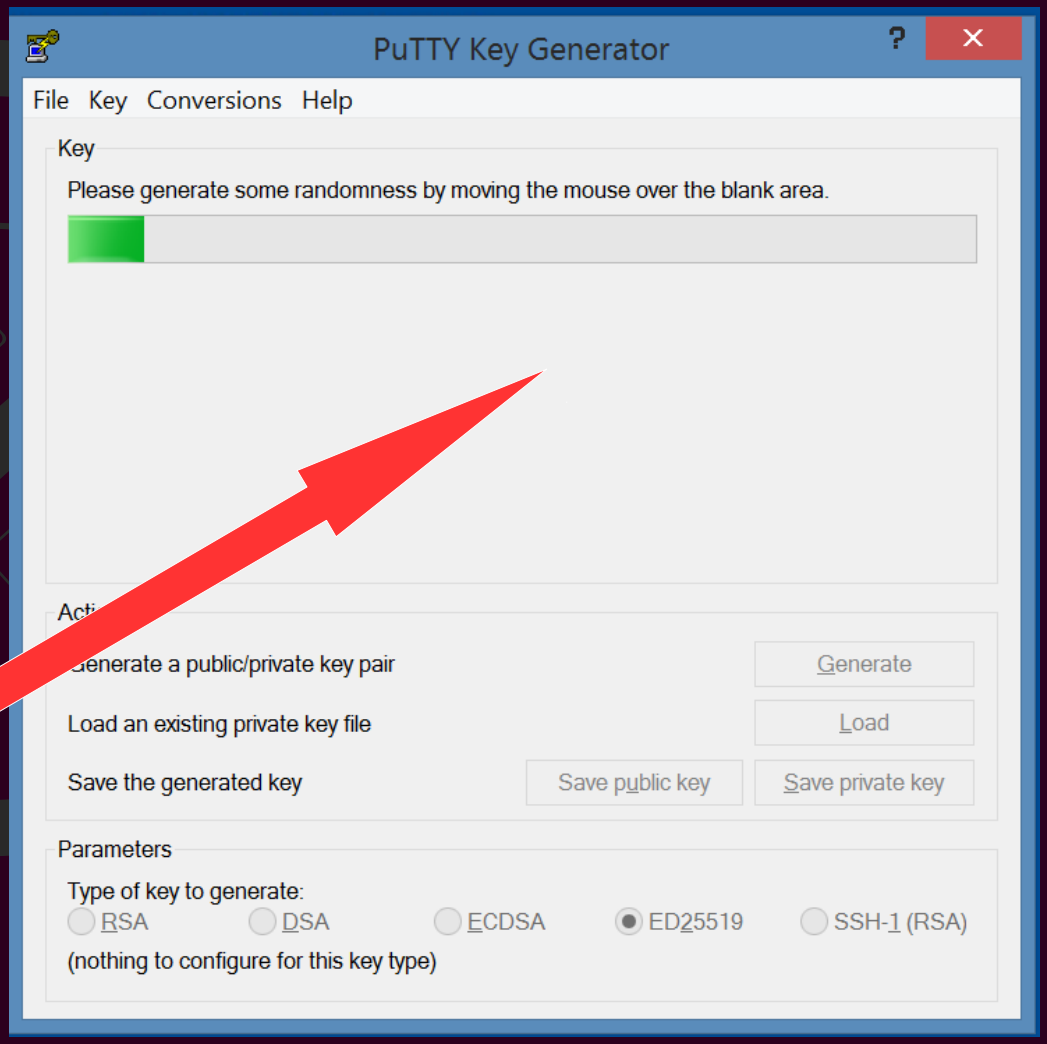
Keys: Generate on Windows

- Install Putty (chiark.greenend.org.uk)
- Start menu → All Programs → PuTTY → PuTTYgen
- Choose “ED25519” and click “Generate”



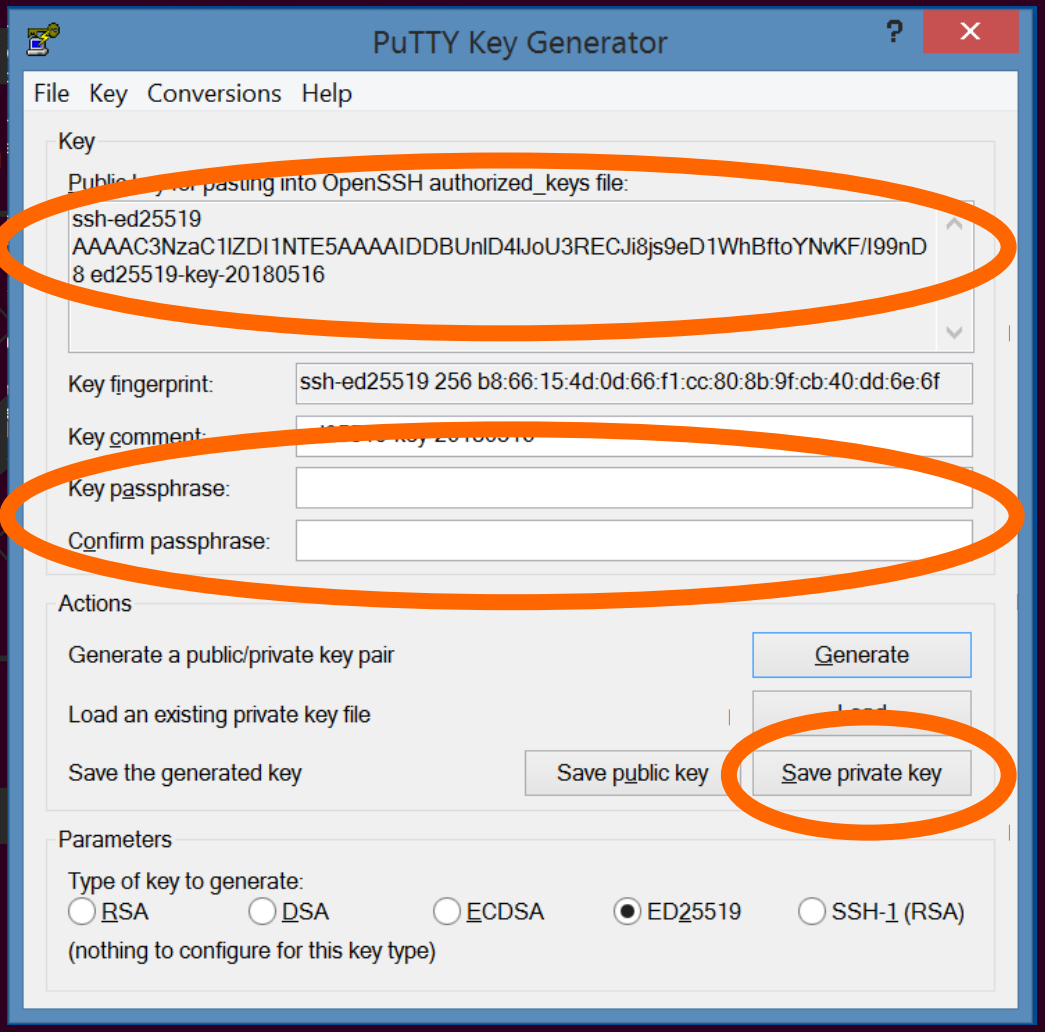
Keys: Generate on Windows

- Install Putty (chiark.greenend.org.uk)
- Start menu → All Programs → PuTTY → PuTTYgen
- Choose “ED25519” and click “Generate”
- Move mouse



Keys: Generate on Windows

- Install Putty (chiark.greenend.org.uk)
- Start menu → All Programs → PuTTY → PuTTYgen
- Choose “ED25519” and click “Generate”
- Move mouse
- Enter password and save priv key
- Copy and paste public key




USE

Use: OMG Security!

- Secure devices with password
- Lock after a timeout
- Full disk encryption
- Different password for every service
- Password safe
- Two factor authentication.

Use: Installing on Your Server

- MacOS/Linux: `ssh-copy-id`

```
ssh-copy-id -i ~/.ssh/priv_key
mrjones-box@nexus.synshop.org
```

Use: Installing on Your Server

- Windows: Manually
- Connect with Putty using password
- Then:

```
mkdir ~/.ssh
chmod 0700 ~/.ssh
touch ~/.ssh/authorized_keys
chmod 0644 ~/.ssh/authorized_keys
nano ~/.ssh/authorized_keys
```

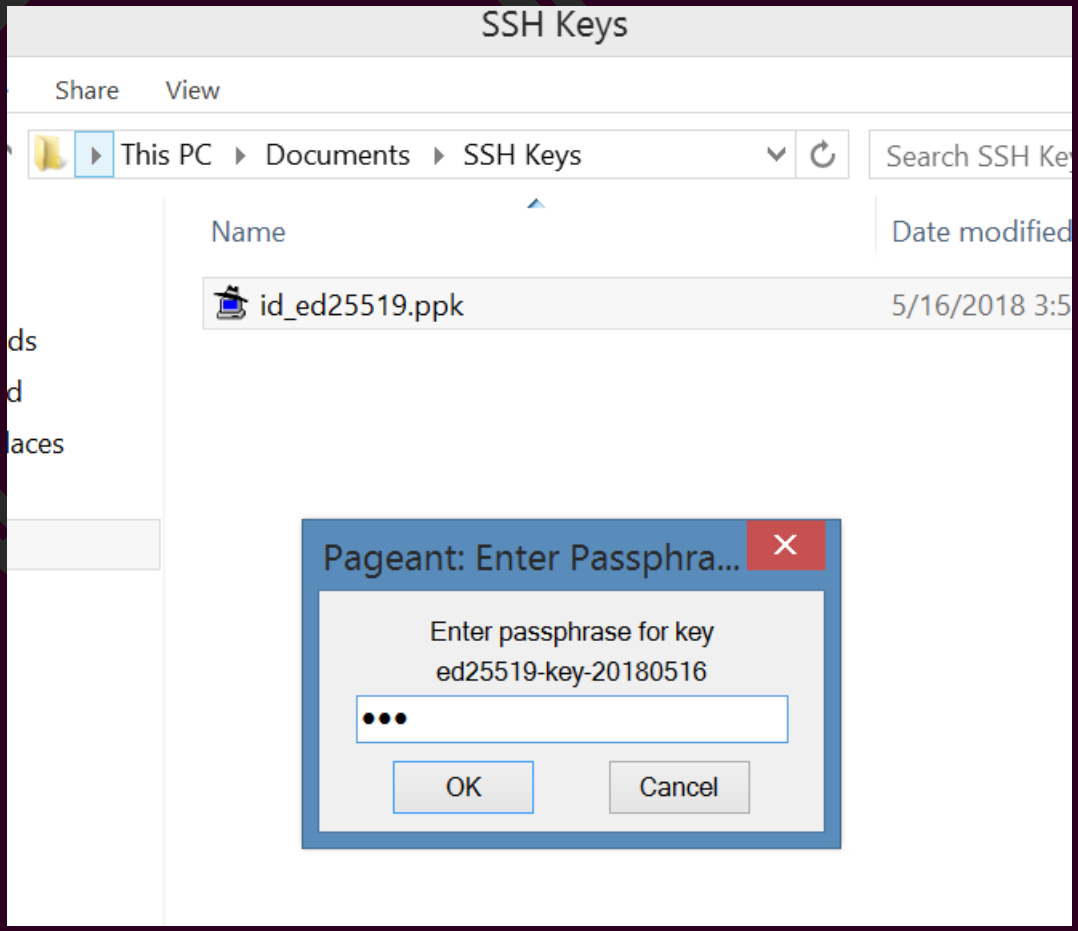
Use: Installing on your free VM

- Email mrjones@plip.com with ***PUBLIC*** key
- Wait for email back with instructions:

```
Have the owner of mrjones-box try
this from outside the shop:

   ssh mrjones-box@nexus.synshop.org

And inside the shop this:

   ssh ubuntu@10.0.40.70
```

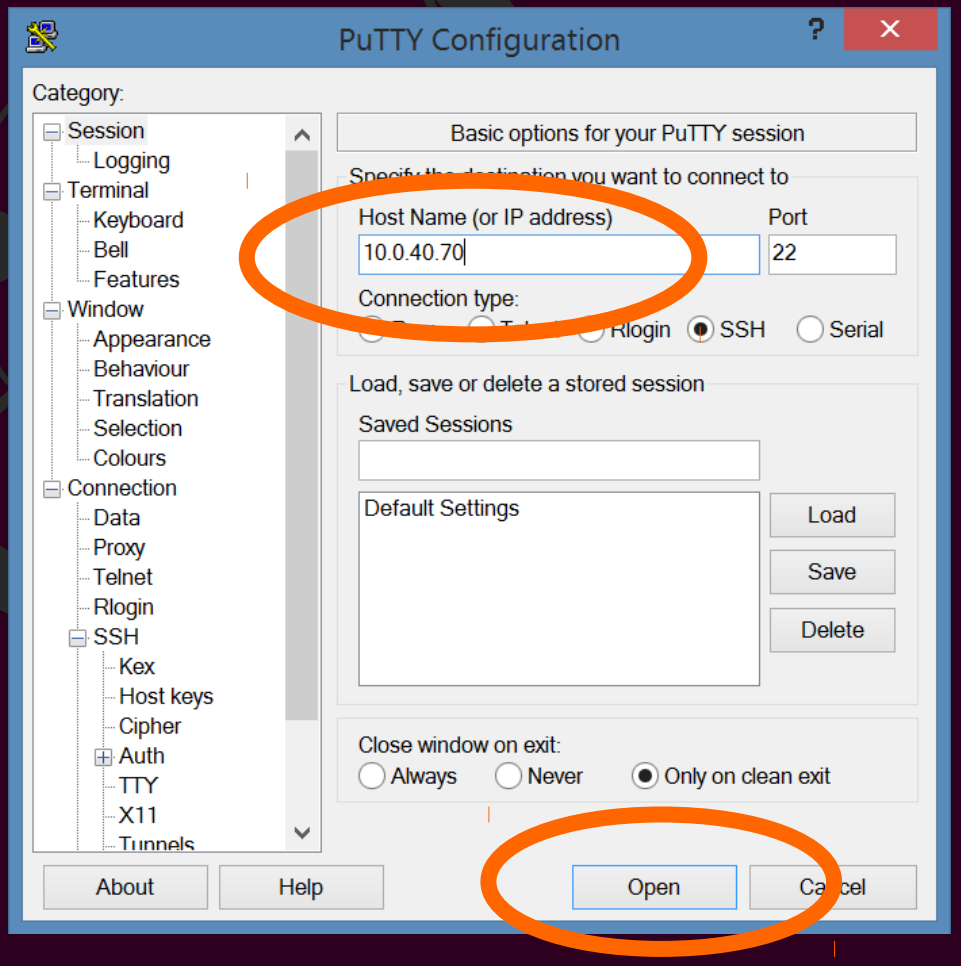
Use: How to connect

- MacOS/Linux: `ssh ubuntu@10.0.40.70`
- Windows:
  1) Add key



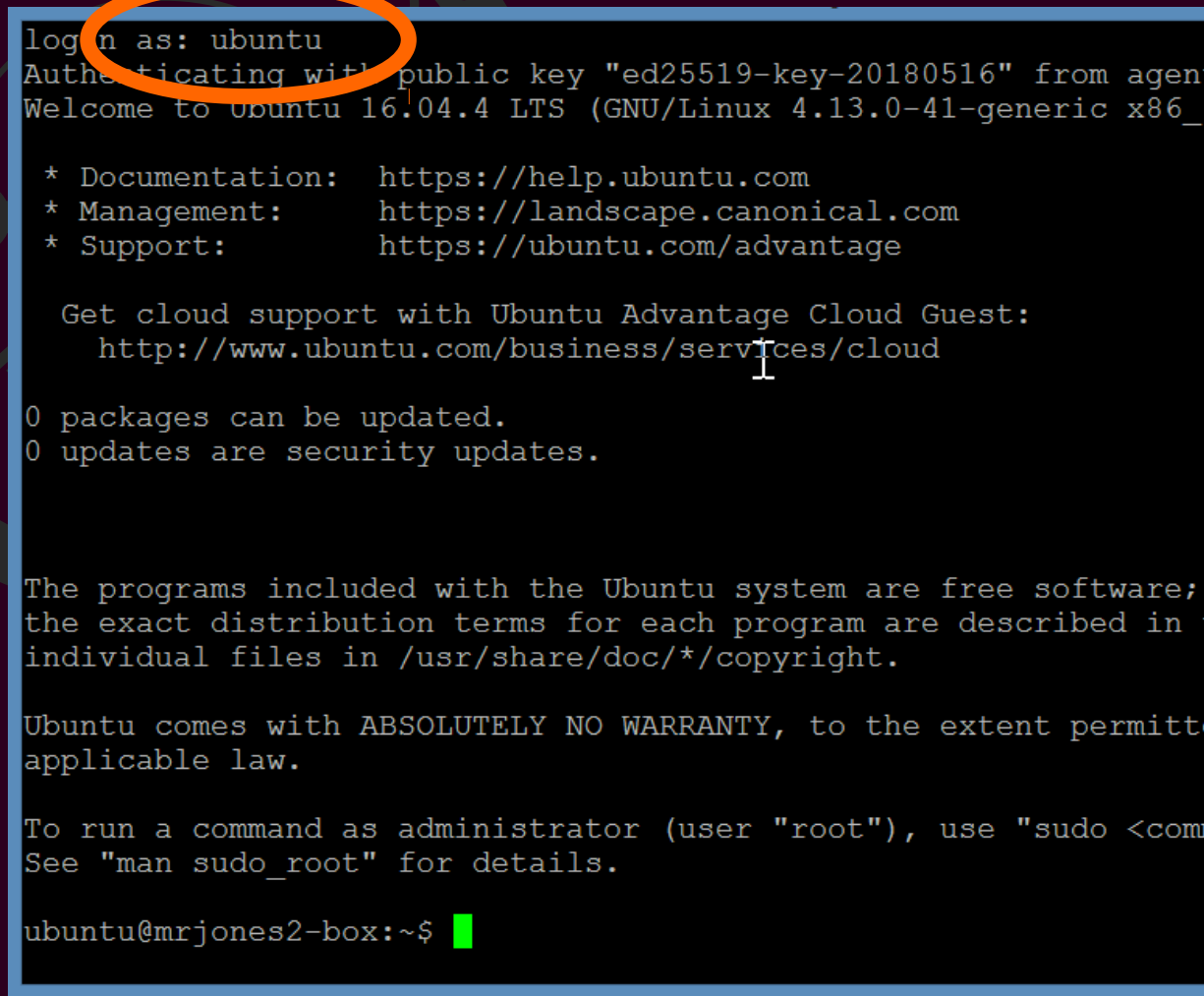
Use: How to connect

- MacOS/Linux: `ssh ubuntu@10.0.40.70`
- Windows:
  1) Add key
  2) Open putty and enter IP, click “Open”



Use: How to connect

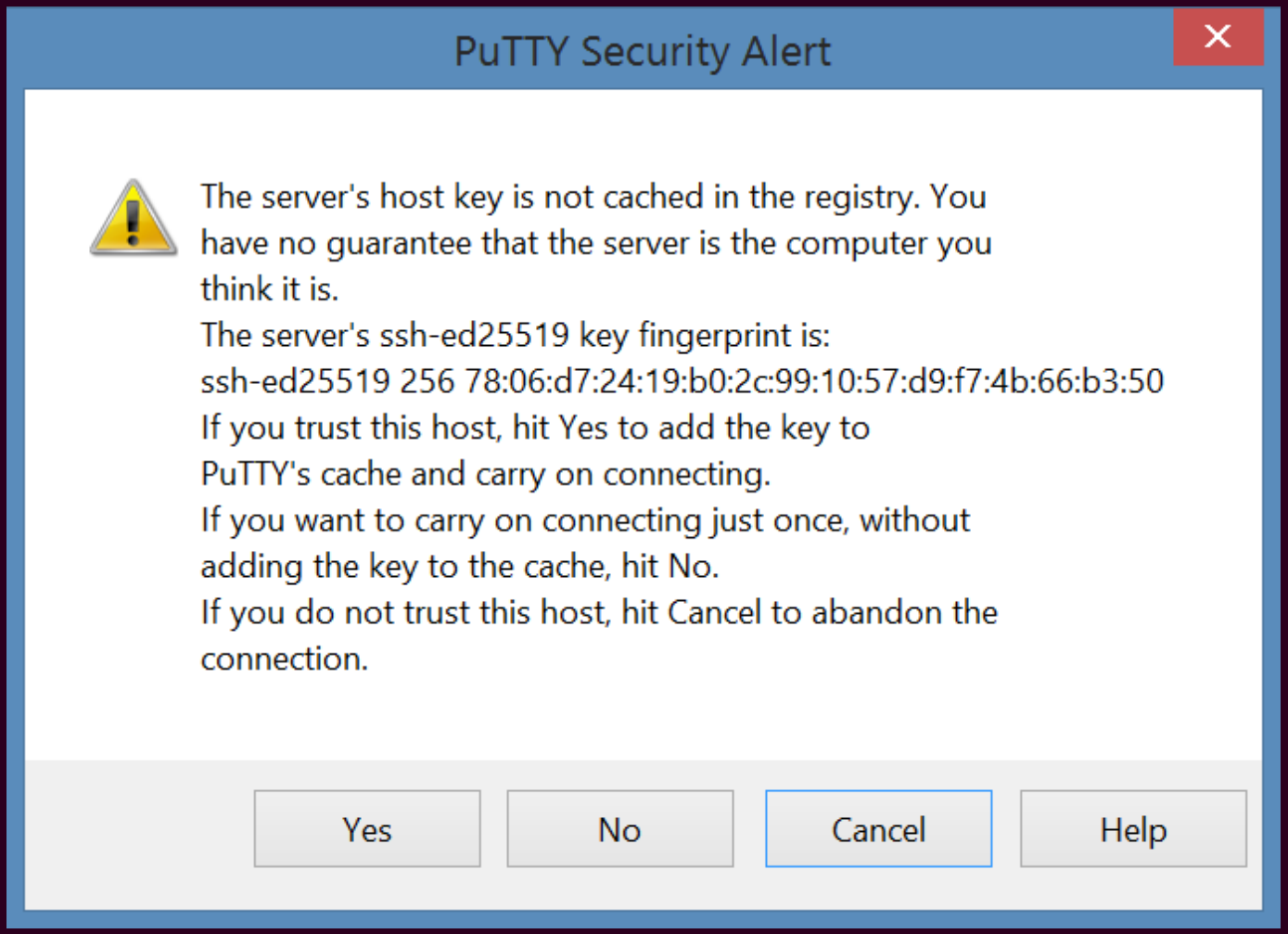
- MacOS/Linux: `ssh ubuntu@10.0.40.70`
- Windows:
  1) Add key
  2) Open putty and enter IP, click “Open”
  3) Login as “ubuntu”



Use: First Time Connect VERIFY!

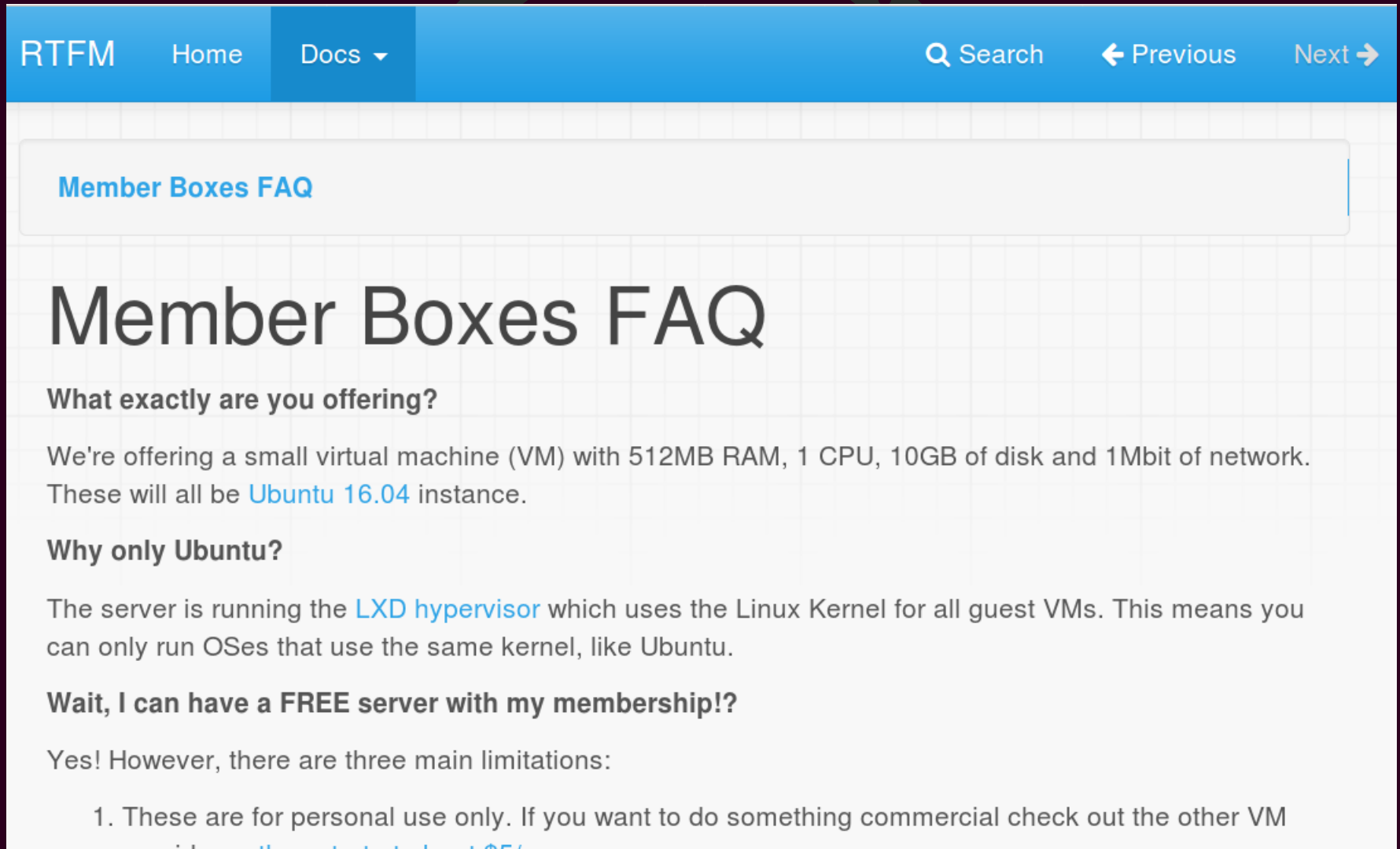
```
ssh ubuntu@10.0.40.70
The authenticity of host '10.0.40.70
(10.0.40.70)' can't be established.
ECDSA key fingerprint is
SHA256:vrdu5rgcUXgzyj75EEd+ER7QU.
Are you sure you want to continue
connecting (yes/no)?
```

Use: First Time Connect VERIFY!



USE: rtfm ;)

rtfm.synshop.org



Thanks! Questions?

mrjones

mrjones@plip.com

plip.com/sshkeys

References

- https://en.wikipedia.org/wiki/Telnet
- https://en.wikibooks.org/wiki/OpenSSH
- https://commons.wikimedia.org/wiki/File:SSH-sequence-password.svg
- https://www.digitalocean.com..understanding-ssh-encryption-connection
- https://en.wikipedia.org/wiki/Secure_Shell
- https://www.slideshare.net/shahhe/introduction-to-ssh
- https://www.ssh.com/ssh/putty/windows/puttygen
- https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
- https://www.ssh.com/ssh/copy-id
- https://askubuntu.com/a/644486
- https://en.wikipedia.org/wiki/Dynix_(software)
- https://www.digitalocean.com/community/tutorials/how-to-use-ssh-keys-with-putty-on-digitalocean-droplets-windows-users
- https://rtfm.synshop.org/docs/lxd-member-boxes/member-boxes-faq./