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 Secure Shell



Tech Review: Features & Uses

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

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



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



3.Connection Layer- Shell can be used



Transport layer
 Authentication layer
 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

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

- .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

- .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!

- .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!

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

RSA Public key – Safe to send anywhere!

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

ed25519 Private key – DO NOT SHARE! KEEP SAFE!

- .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!

- .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

- .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: ed25519 type

cat /tmp/deleteme

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

B3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAABAAAAAAAAAAAAAAAAAAAAA QyNTUxOQAAACCNSQA33K+EGj5HbswDVyTHqnomHBL/XgVYPhDdAor0EwAAAJi3fsk0t37J NAAAAAtzc2gtZWQyNTUxOQAAACCNSQA33K+EGj5HbswDVyTHqnomHBL/XgVYPhDdAor0E AAAEAA957sXvHPYfUTczho/7TCY3Xppau36YbqoBEJ1JFVg41JADfcr4QaPkduzANXJMeq eiYcEv9eBVg+EN0CivQTAAAAEG1yam9uZXNAYWlyYnVudHUBAgMEBQ==

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

cat /tmp/deleteme.pub

ssh-ed25519
AAAAC3NzaC11ZDI1NTE5AAAAII1JADfcr4QaPkduzANXJMeqeiYcEv9eBVg+EN0CivQT
mrjones@airbuntu

Keys: rsa type

cat /tmp/deleteme

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

MIIJKAIBAAKCAqEAwUlqeHfMOBiMaLZCU5AnqG4Mq/l0ewE0DrKBFlAmy3W0LeWq WKG+ZzVOgyJX8GWs0OLzaM1LZBrURTb4EXAOdzvGmMUmoP1GKO4BanpKaEEStKe1 iuokdqH97hFBc7fpBp6bB179FG0705IOGfqCmMMhMgTyNmX7RRokUwAEDvEaS8rI 01xxfiqOEapce7c8c1Z4HPpqNZhYK1zfbEQKDB9salAlHj5qc1jtScHFSEG3Q7vD ZLj6Kq1DobASfL/6f5vEn+PBCvSRw2hQE12VfX16P7pn210xd+Sd4wz4Zf1swX2b fjc/tLZXAknsiiznITZf41kNJ1j1/QB6dXhdhVs16BxYktS9fpY4sPbNmx31E/0I 1hCdwm76qqPPGWnpUajKubpeiafGaw3p2CJBAOyqmpiU6x60V+B54LZDysjHvwbB +3mDsjvScQE36flq9vdRk4QH/Seq+ZFqhLhc/04vT9qGCLrLiSP1L3rhd1cEpMVc mA+XhMnnBF1BpSWZFK2CWTHkdidts3QEjNVxjjZ0X6nO4u0B83Pp1XpUvdmoPCuU btMpXnmzuENhUZjJWXex2ESzVcAfJTn8cr9ecVJQQnEfwkCPCddSwBuXS/0tTXcD 0yCrKcrvmBRrMb+AlmL76BDPNcqX8GE5A4/8QoEfVRmNUIFHHNX8rr0jCncCAwEA AOKCAgAHtlzSEb21U11u5C7bVLouxrVbIr4CFnc0Su0ZrdMOdUDeP/a/GJ0XUyoz a+hkYDo4EM0TlkyazvM/W8UkNPtuyITRHbS/4btF8hgeXojPhiEv8i0tQNB5p1cR g8C/1EvJBtUawzCH+x/S/1XvtVStMcOGUeo0P3d6N2PRgAOBcR9ifNHs1Ri2Nw56 J/kOuq3/0Ch0x40rXEvQVyFXGZPpDevuhqolHcpzi5bURZYQnwan/jr6ruLUhxtW vUbPkX12UAnVc2oFfOLAEE55p1dKrZIOLurr7KIHraibIa5bq0sqoU9uBthU5p2s KrT0qnwqeBf1Y11B/6u5D6bTPx1EHqz7LX5zL93inAPLRy18tdXizXXisL1Ec1vm Ha5bXVnUYWZmrqOosqjOcscxXOeOwE63cxWOhpuN9G3kuXLuqZrWnKzFPZX+/zM5 0+pD4QKCAQA4020jmb+vyFfq15PG/Z3btBQFfIfq7QFsArsCx+4jf1xFMoe3qWaa 37Ls7RZALskN3ILyosm4oWNORrg8kbi9Q6eNifEw0lDbOWZeslbqwJWNhN6/EIL2 PGQSXaqjyVsk0MaD0T2GKfBsFbSN9X1q8MNjN2/oHVowZu5qaRmrjpgkxph0MT02 UcwVLrzVc5iXFcAGjGGc1GCsfRoNo5iZo/o4KIW0m3BTOzr/O+DJmIEiLCN3hOYM SPG9rekR4jyfGeq1MlM+Zfd5q1s+6Pq6v4qKUzW7KWlGiJvHqlEvRXG12q41XZIp qMn/EmQ2aU+H/C+tb5yIayYy7qWHu8z/AoIBACsySqzfXGWy4Pxyw34IHhLdQ305 JEMwx3wSx15lnUk4oGLAo2fjFqfbMMwFFXbIni7mxaKU3wjTHQSBKDEZoUQXYx5s WCs3B2anPNnRZ/V7Gty/fJaVsdlyW8n3+b67MvtkjpR7PwIkIcqY9nBTMvWmJM73 94Y1WW6xB2V6trAJMxVYnTWbqmYZZI76L6GOBTWZmOQlqVKysfuc5fNqz4h/9sQv AD7HNvas1Fi6TqDAH4E91osDnhIXKq/+fIKqxVxXlydruY018+Bzoj803HD4BkW0 z2sHtxywGGN5rIfPzOA5r3cmWxdPFhe0JmR2cyug8H8NKw1Z9ZCkVdaszw=

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

→ ~ cat /tmp/deleteme.pub

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDBSWB4d8w4GIxotkJTkCeAbgyD+XR7ATQOsoEWUCbLdbQt5apYob5nN U6rIlfwZazRAvNoyUtkGtRFNvgRcA5308aYxSag/UYpDgFqekpoQRK0p7WK6iR2of3uEUFzt+kGnpsHXv0UbTvTkg4Z+ AKYwyEyBPI2ZftFGiRTAAQ08RpLysjTXHF+Ko4Rqlx7tzxzVngc+mo1mFgrXN9sRAoMH2xqUCUePmpyWO1JwcVIQbdDu 8NkuPoqrUOhsBJ8v/p/m8Sf48EK9JHDaFATXZV9fXo/umfaXTF35J3jDPh1+WzBfZt+Nz+0tlcCSeyKLOchN1/jWQ0nW PX9AHp1eF2FWzXoHFiS1L1+1jiw9s2bHfUT/QjWEJ3Cbvqqo88ZaelRqMq5u16Jp8ZrDenYIkEA7KqamJTrHo5X4Hngt kPKyMe/BsH7eYOyO9JxATfp+WD291GThAf9J6D5kWqEuFz/Ti9P2AYIusuJI/UveuF3VwSkxVyYD5eEyecEXUG1JZkUrY JZMeR2J22zdASM1XGONnRfqc7i7QHzc+mVelS92ag8K5Ru0yleeb04Q2FRmM1Zd7HYRLNVwB81Ofxyv15xU1BCcR/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]--+ • • • • . .0 .

E0.0 .

o oo^o=

++*=@

+----[SHA256]----+

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

| E PuT | TY Key Generator | ? × |
|---|---------------------------------------|--------------------------|
| File Key Conversions Help Key No key. | | |
| Actions Generate a public/private key pair Load an existing private key file | [| <u>G</u> enerate Load |
| Save the generated key | Save p <u>u</u> blic key | <u>S</u> ave private key |
| Parameters Type of key to generate: <u>RSA</u> (nothing to configure for this key type | ● <u>ECDSA</u> ● <u>ED25519</u> e) | ○ SSH- <u>1</u> (RSA) |

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

| E | PuTTY Key | Genera | ator | ? | × |
|---|-----------|--------|---------------------|------------------------|------|
| File Key Conversions Help Key No key. | | | | | |
| | | | | | |
| | | | | | |
| Actions | | | | | |
| Generate a public/private key p | pair | | | <u>G</u> enerate | |
| Load an existing private key file | e | | | Load | |
| Save the generated key | | Save | p <u>u</u> blic key | <u>S</u> ave private k | ey |
| Parameters | | | | | |
| Type of key to generate: <u>R</u> SA <u>D</u> SA | | SA | • ED25519 |) SSH- <u>1</u> (F | RSA) |
| (nothing to configure for this keep | ey type) | | | | |

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

| 3 | | | P | uTTY Key | Generator | ? × |
|------|---------------|--------------------|-------------|---------------|------------------------|--------------------------|
| File | Key | Conversions | Help | | | |
| Ke | ey | | | | | |
| F | lease | generate some | randomne | ess by moving | the mouse over the bla | nk area. |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| A | cti | | | | | |
| | aenera | ite a public/priva | ite key pai | r | | <u>G</u> enerate |
| L | oad a | n existing private | e key file | | | Load |
| 5 | Save th | e generated ke | y | | Save public key | <u>S</u> ave private key |
| Pa | aramet | ers | | | | |
| Т | ype of | key to generate | e: | | | |
| |) <u>R</u> S/ | | <u>)</u> SA | <u> </u> | SA • ED <u>2</u> 5519 | SSH- <u>1</u> (RSA) |
| (| nothing | g to configure fo | or this key | type) | | |

- 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

| 70 2 | PuTTY Key | Generator | ? 🗙 | | | | |
|---|--|--|-----------------------|--|--|--|--|
| File Key Conversions | Help | | | | | | |
| Key | | | | | | | |
| Public L, pasung Ir | nto OpenSSH authorize | d_keys file: | | | | | |
| ssh-ed25519 AAAAC3NzaC1IZDI1N 8 ed25519-key-201803 | ssh-ed25519 AAAAC3NzaC1IZDI1NTE5AAAAIDDBUnID4IJoU3RECJi8js9eD1WhBftoYNvKF/I99nD 8 ed25519-key-20180516 | | | | | | |
| | | | × 1 | | | | |
| Key fingerprint: | ssh-ed25519 256 b8:6 | 6:15:4d:0d:66:f1:cc:80:8 | b:9f:cb:40:dd:6e:6f | | | | |
| Key <u>c</u> omment- | 2010001 | U Contraction of the second se | | | | | |
| Key p <u>a</u> ssphrase: | | | | | | | |
| Confirm passphrase: | | | | | | | |
| Actions | | | | | | | |
| Generate a public/priva | ate key pair | [| <u>G</u> enerate | | | | |
| Load an existing private | e key file | | Land | | | | |
| Save the generated key Save p <u>u</u> blic key <u>Save private key</u> | | | | | | | |
| Parameters | | | | | | | |
| Type of key to generate | e: SA O <u>E</u> CDS | 6A • ED <u>2</u> 5519 |) SSH- <u>1</u> (RSA) | | | | |
| (nothing to configure for | or this key type) | | | | | | |



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

| SSH Keys | | | | | |
|------------|-----------|---|--------|---------------|--|
| Share | View | | | | |
| 📜 🕨 Thi | s PC → Do | cuments 🕨 SSH Keys | ✓ C | Search SSH Ke | |
| | Name | • | | Date modified | |
| | 🏂 id_ | ed25519.ppk | | 5/16/2018 3:5 | |
| d laces | | Pageant: Enter Passphr | a × | | |
| | | Enter passphrase for ke ed25519-key-20180516 ••• OK Canc | y S | | |

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"

log n as: ubuntu Authe ticating with public key "ed25519-key-20180516" from agen Welcome to upuntu 16.04.4 LTS (GNU/Linux 4.13.0-41-generic x86

- * Documentation: https://help.ubuntu.com Management:
- * Support:
- https://landscape.canonical.com https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest: http://www.ubuntu.com/business/services/cloud

packages can be updated. updates are security updates.

The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitt applicable law.

To run a command as administrator (user "root"), use "sudo <com See "man sudo root" for details.

ubuntu@mrjones2-box:~\$

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!

х **PuTTY Security Alert** The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is. The server's ssh-ed25519 key fingerprint is: ssh-ed25519 256 78:06:d7:24:19:b0:2c:99:10:57:d9:f7:4b:66:b3:50 If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting. If you want to carry on connecting just once, without adding the key to the cache, hit No. If you do not trust this host, hit Cancel to abandon the connection. Yes No Cancel Help

USE: rtfm ;)

rtfm.synshop.org

| RTFM | Home | Docs 🗸 | Q Search 🔶 Previous | Next 🔶 |
|---------|------------|--------------|---------------------|--------|
| Membe | er Boxes F | FAQ | | |
| Me | mb | er Bo | oxes FAQ | |
| What ex | actly are | you offering | | |

We're offering a small virtual machine (VM) with 512MB RAM, 1 CPU, 10GB of disk and 1Mbit of network. These will all be Ubuntu 16.04 instance.

Why only Ubuntu?

The server is running the LXD hypervisor which uses the Linux Kernel for all guest VMs. This means you can only run OSes that use the same kernel, like Ubuntu.

Wait, I can have a FREE server with my membership!?

Yes! However, there are three main limitations:

1. These are for personal use only. If you want to do something commercial check out the other VM

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-puttyon-digitalocean-droplets-windows-users
- https://rtfm.synshop.org/docs/lxd-member-boxes/member-boxes-faq./