Everything SSH!

September 2019 Jeffery Russell

RITLUG

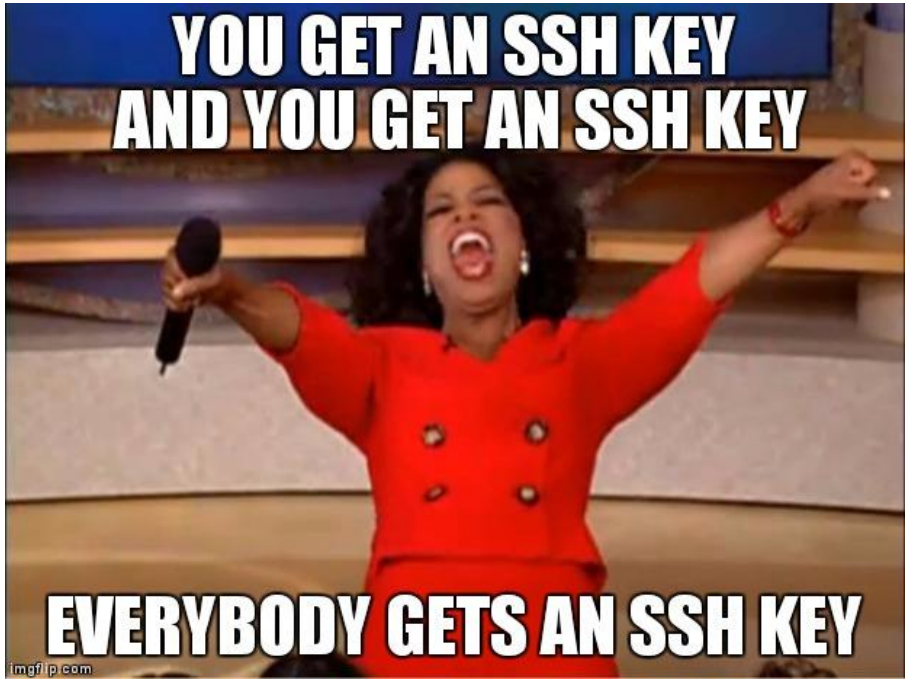
ritlug.com

Please sign in!

signin.ritlug.com

Keep up with RITlug outside of meetings:

ritlug.com/get-involved, rit-lug.slack.com

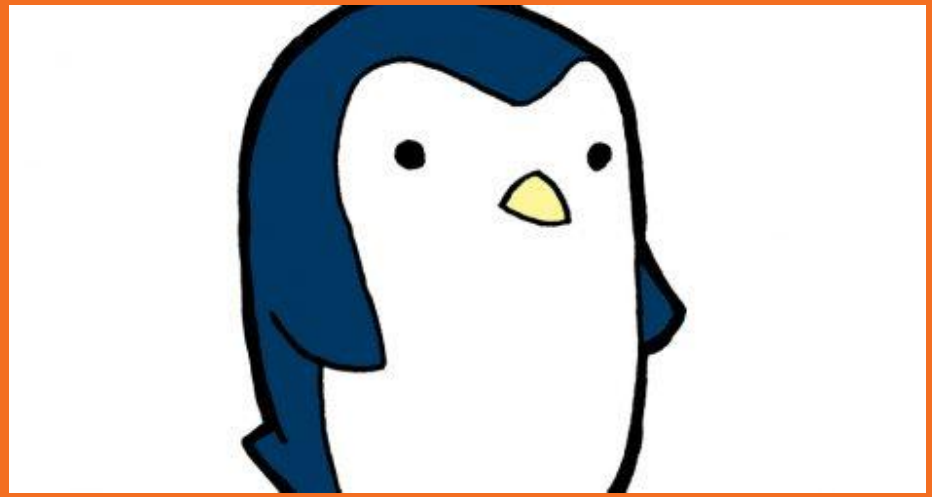


What is SSH?

SSH is...

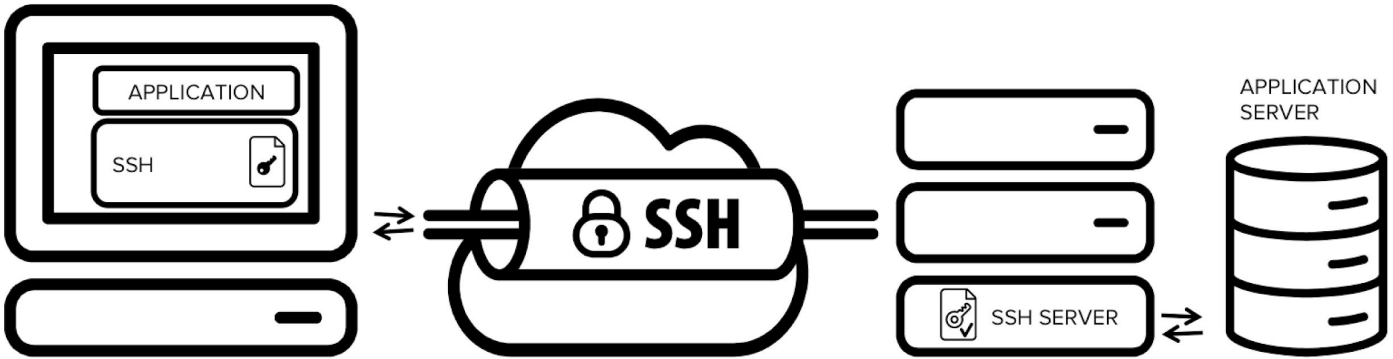
- AKA: Secure Socket Shell
- Open source tool used for connecting to a remote computer in a secure manner
- Version 1 developed in 1995 and second version developed in 2006
- Authentication with Diffie-Hellman key exchange

WHY?



SSH is powerful...

- SSH makes connecting to remote computers **very easy**
- Widely implemented
- Supports a plethora of features:
  - Passwordless login with keys
  - File transfer
  - Network port forwarding
  - SSH config files



HOW?

Just pop open a terminal!

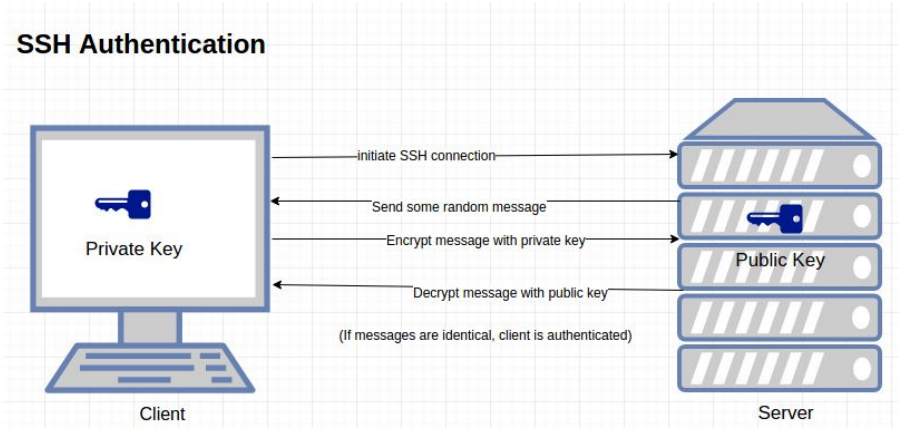
- Command syntax
  - ssh user@hostname -p port -i keyFile
- The default port used for ssh is 22
- If no user is provided, it will use your current user name

```
┌─[jeff@jrtechs-laptop] - [~] - [2019-09-03 07:51:32]
└─[1] <> ssh jxr@glados.cs.rit.edu
The authenticity of host 'glados.cs.rit.edu (129.21.22.196)' can't be established.
ECDSA key fingerprint is SHA256:pbfV7PlN905l5ubqUckN2ahZ2iJ9TCG/DGPVxDgMgek.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'glados.cs.rit.edu,129.21.22.196' (ECDSA) to the list of known hosts.
Password:
```

Keys!

Keys!

- Keys allow you to log into an SSH server without a password.
- SSH uses a public-private key pairing
  - Private key is kept on local machine
  - Public key is distributed to the remote computer

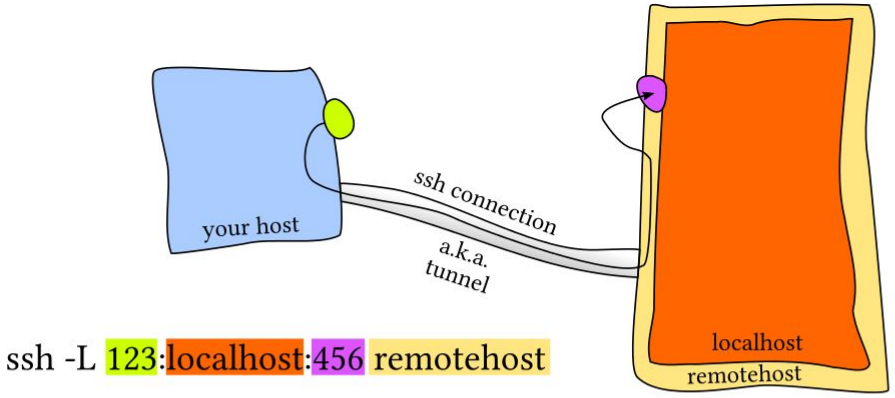


Commands

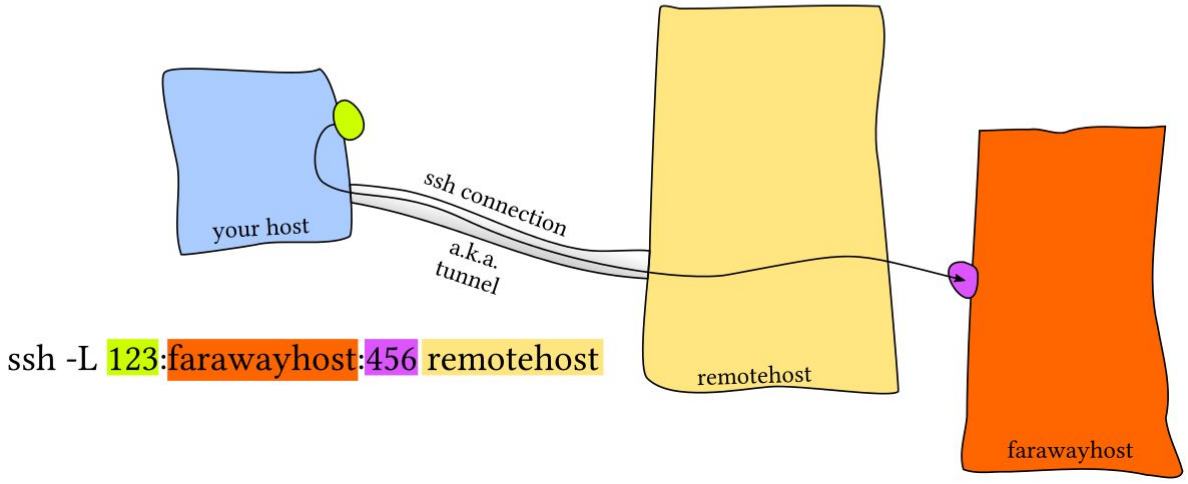
- ssh-keygen
  - Generates new key pair
- ssh-copy-id
  - Copies your public key to remote server
- ssh-add
  - Adds a private key to the list of keys that ssh will try to connect to remote servers with by default

Local Port Forwarding

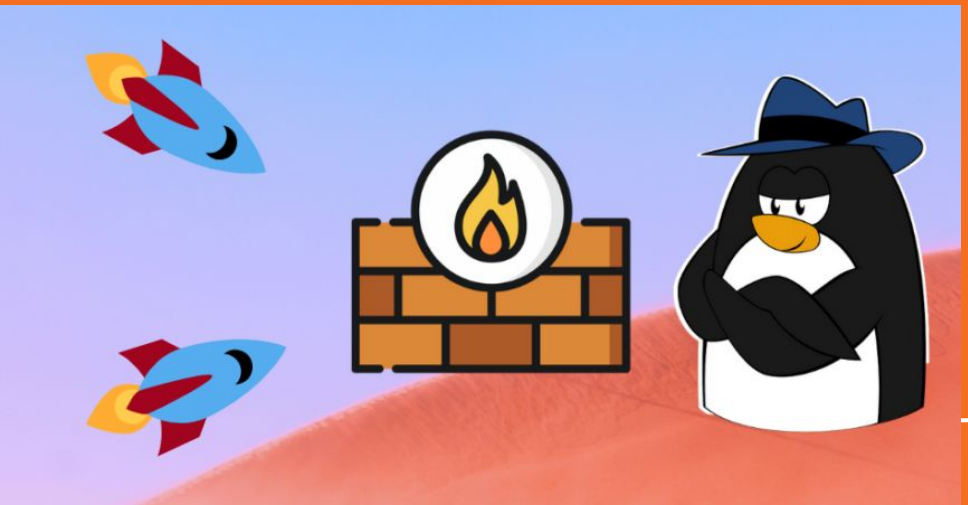
Local Port forwarding



- Allows you to forward traffic from a port on your computer to a remote destination available to a remote computer.
- Often used to access remote web servers or resources that are behind a firewall.

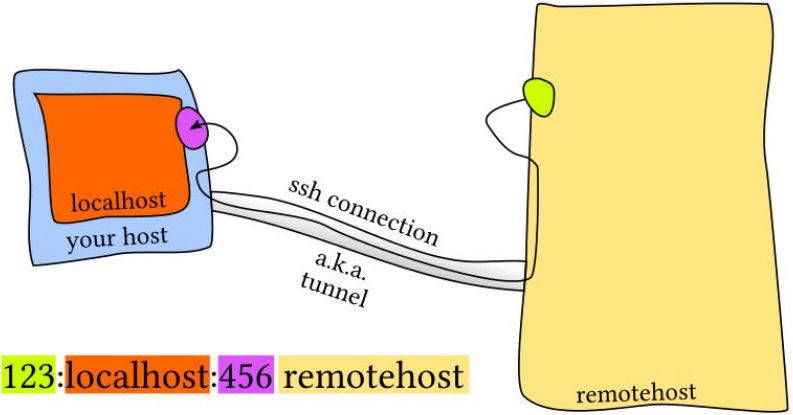


Remote Port Forwarding

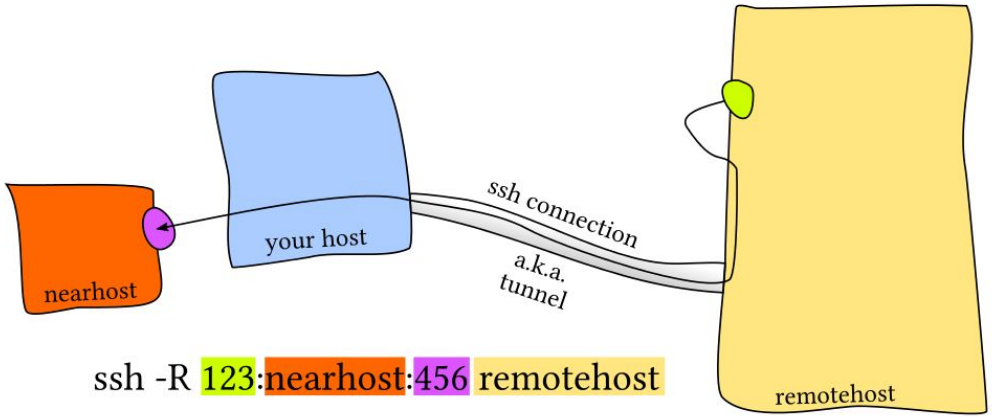


Remote Port Forwarding

- Forwards traffic on a remote computer to your local machine.
- Often used to expose dev environment to the internet.




```
ssh -R 123:localhost:456 remotehost
```




```
ssh -R 123:nearhost:456 remotehost
```

Socks Proxies, SSHFS, SFTP, SSH Configs

~/.ssh/config

```
Host dev
    HostName dev.example.com
    User john
    Port 2322
```

Challenge!

Challenge!

Try to be the first one to make it through 5 ssh challenges and change the website demo.ritlug.com

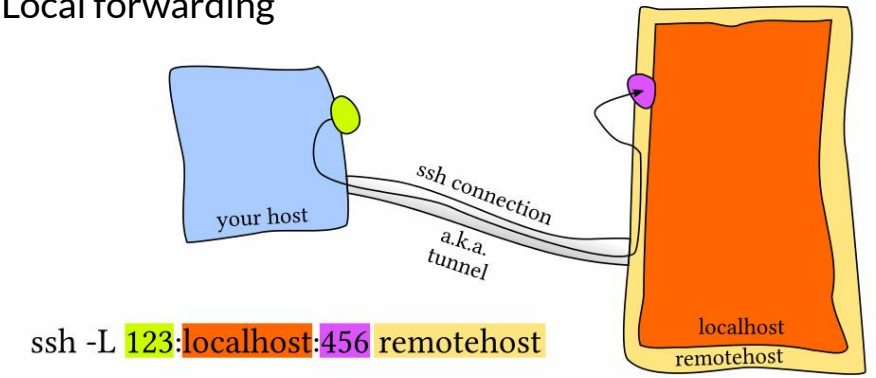
Host: demo.ritlug.com
User: ritlug
Password: ritLugSep6!

Parts of this are difficult, ask for help!

**This host/VM is no longer on but, you can download the challenge on github.

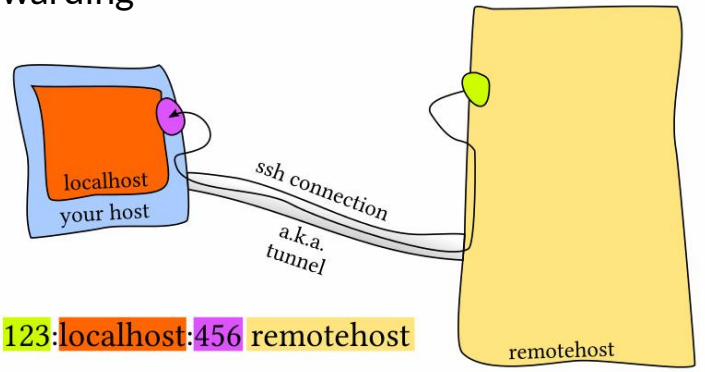
ssh user@hostname -p port -i keyFile

Local forwarding



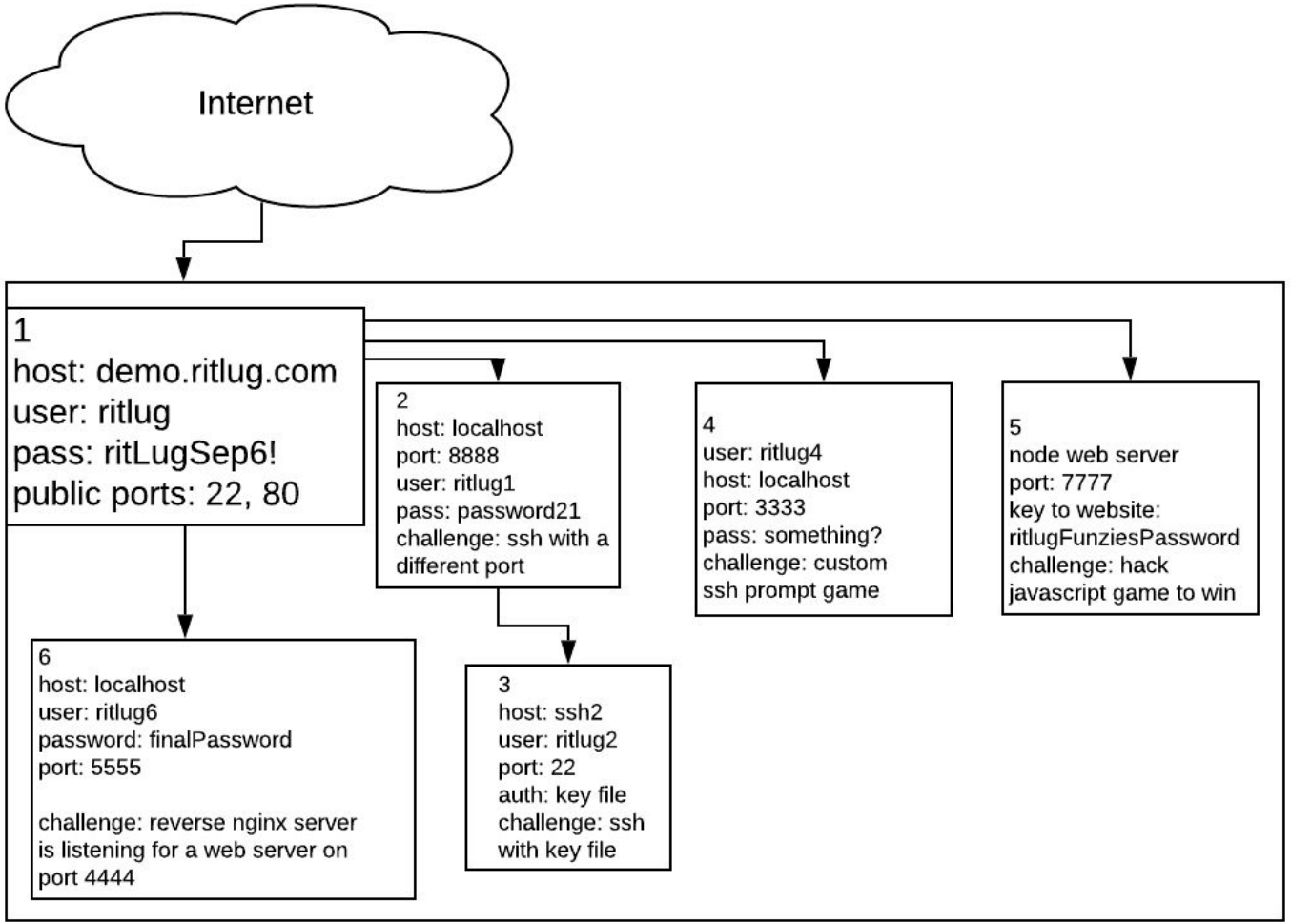
ssh -L 123:localhost:456 remotehost

Remote forwarding



ssh -R 123:localhost:456 remotehost

Challenge Solution Demo


Internet
1
host: demo.ritlug.com
user: ritlug
pass: ritLugSep6!
public ports: 22, 80
2
host: localhost
port: 8888
user: ritlug1
pass: password21
challenge: ssh with a different port
4
user: ritlug4
host: localhost
port: 3333
pass: something?
challenge: custom ssh prompt game
5
node web server
port: 7777
key to website: ritlugFunziesPassword
challenge: hack javascript game to win
6
host: localhost
user: ritlug6
password: finalPassword
port: 5555
challenge: reverse nginx server is listening for a web server on port 4444
3
host: ssh2
user: ritlug2
port: 22
auth: key file
challenge: ssh with key file

Questions

Resources

- SSH Essentials
- SSH Config Files
- Git Repo and Write Up for Challenge