

# **Unit 2: Welcome to your home**

## **SSH Fundamentals**

Lesson 14

Derek Ruths

# Overview of unit

Objectives:

- Fundamentals of working in UNIX
- Fundamentals of working in the cloud

1. Why UNIX?
2. Why AWS and the Cloud?
3. Setting up a UNIX VM
4. SSH
5. Key-based Auth
6. Basic UNIX commands & admin
7. Installing python
8. Intermediate UNIX tools
9. Working remote
10. Text editors
11. Advanced customization
12. HW 2

# Lesson overview

## Objectives

- Understand the use and configuration for ssh
- Understand public-private keys
- Setup access to your EC2

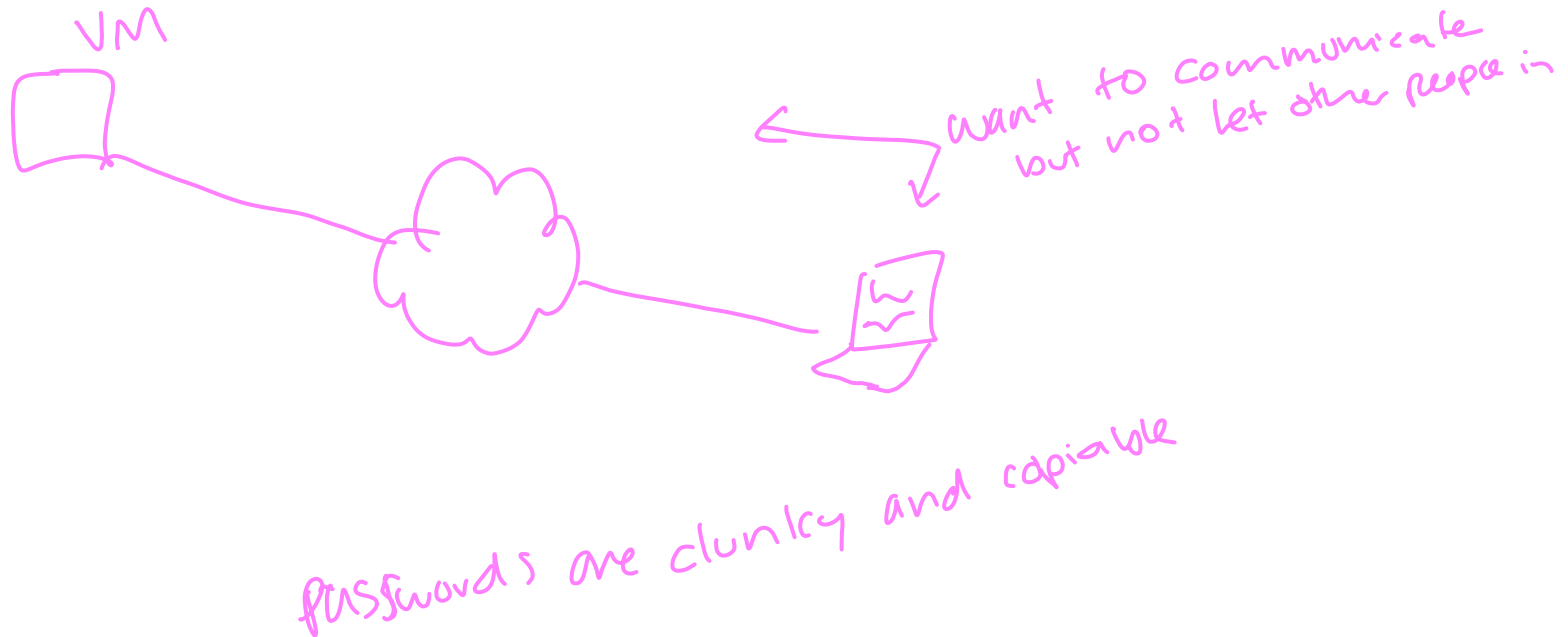
## Outline

- How does ssh work?
- How does public-private cryptography work?
- Setting up your ssh client to access your EC2 instance

# How does SSH work?

- SSH = “secure shell”
- A way to access the (UNIX) command line on another computer

# The authentication problem



# Public-private key cryptography



combo lock

only one person  
knows the code  
but lots of people  
can handle the  
lock

public-private key pair

combine:  $(K_p, K_v)$

↑  
combo lock  
(public)

↑  
lock  
(private)

anyone can touch the  
public key, only you have private

# The (high-level) SSH protocol

SSH -i ~/Downloads/Tess370.pem (user)@(publicipaddress)

secure copy  
SCP -i (keypath) (user)@(ipaddress):(file) (destination)  
on home computer

# Demo time



# Lesson wrap-up

## Takeaways

- You can get into your EC2!

## Up next

- Basic UNIX commands & admin