SSH guides

We'll first need to introduce some terminology, definitions, and things you'll interact with.

If you know about SSH, can generate your own ssh-keys, and are familiar with a terminal or shell, you can skip this part.

Terminology

- VM: Virtual Machine. The trainer made one for everyone. We will identify these based on their IP.
- SSH: secure shell. A way to interact with remote systems (such as our VM).
- Authentication: the VM only allows SSH connections from systems it knows. So, you'll need to authenticate.

Keyfiles

1. You will generate your own unique keyfile.
2. You will send this keyfile to your trainer.
3. Your keyfile will be given to your VM, which will then be able to recognize and authenticate your session.

A keyfile consists of two parts:

- A private key. You do *NOT* share this, ever.
- A public key, which you can share. This should have the extionsion `.pub`

Options to connect over SSH

- Linux and Mac have an SSH client built in.
- Windows *usually* does not.
  - PowerShell has a SSH-module (Posh-SSH).
  - Putty is a free SSH (and Telnet) client. There are versions for Linux

and Mac as well.

- Windows Subsystem for Linux allows you to run Linux commands (including SSH) on your Windows system.
- Many more options, use whatever you're comfortable with. We'll discuss the first three.

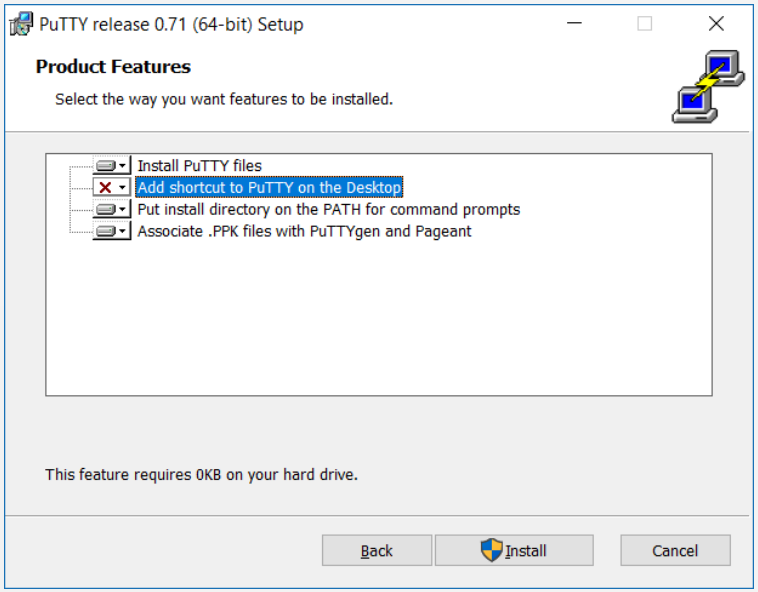
Do you already have SSH?

1. Open a terminal (or PowerShell; WIN+X, A, click `yes`).
2. type `ssh`, and hit `enter`

If you see a response (i.e. not an error), you have SSH! Hang back and wait for everyone else to catch up!

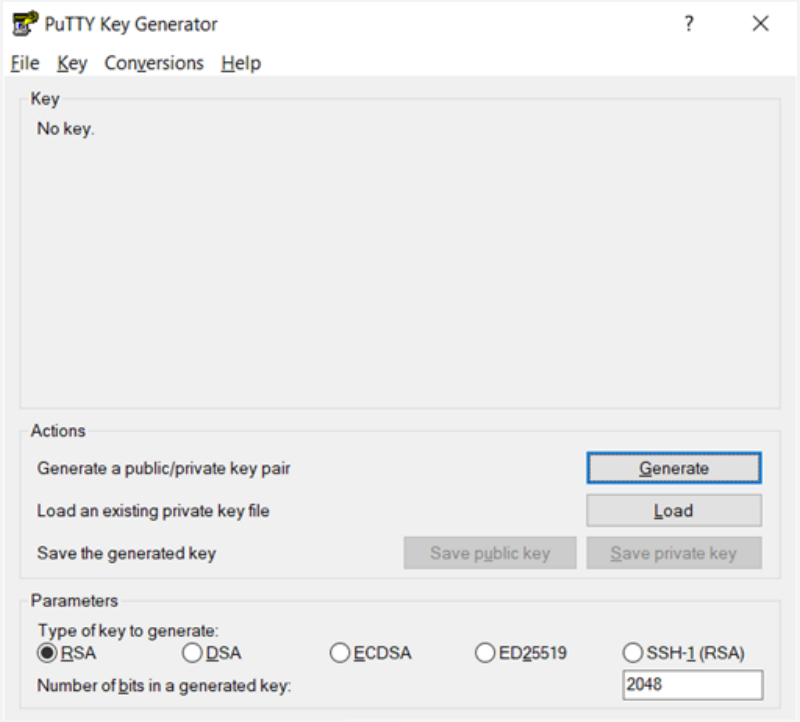
Getting Putty

1. Download Putty (64bit, 32bit)
2. Open the installer, and follow the instructions. Please ensure the features look like this:



SSH keys (PuttyGen)

Open PuttyGen, and hit the 'generate'-button:

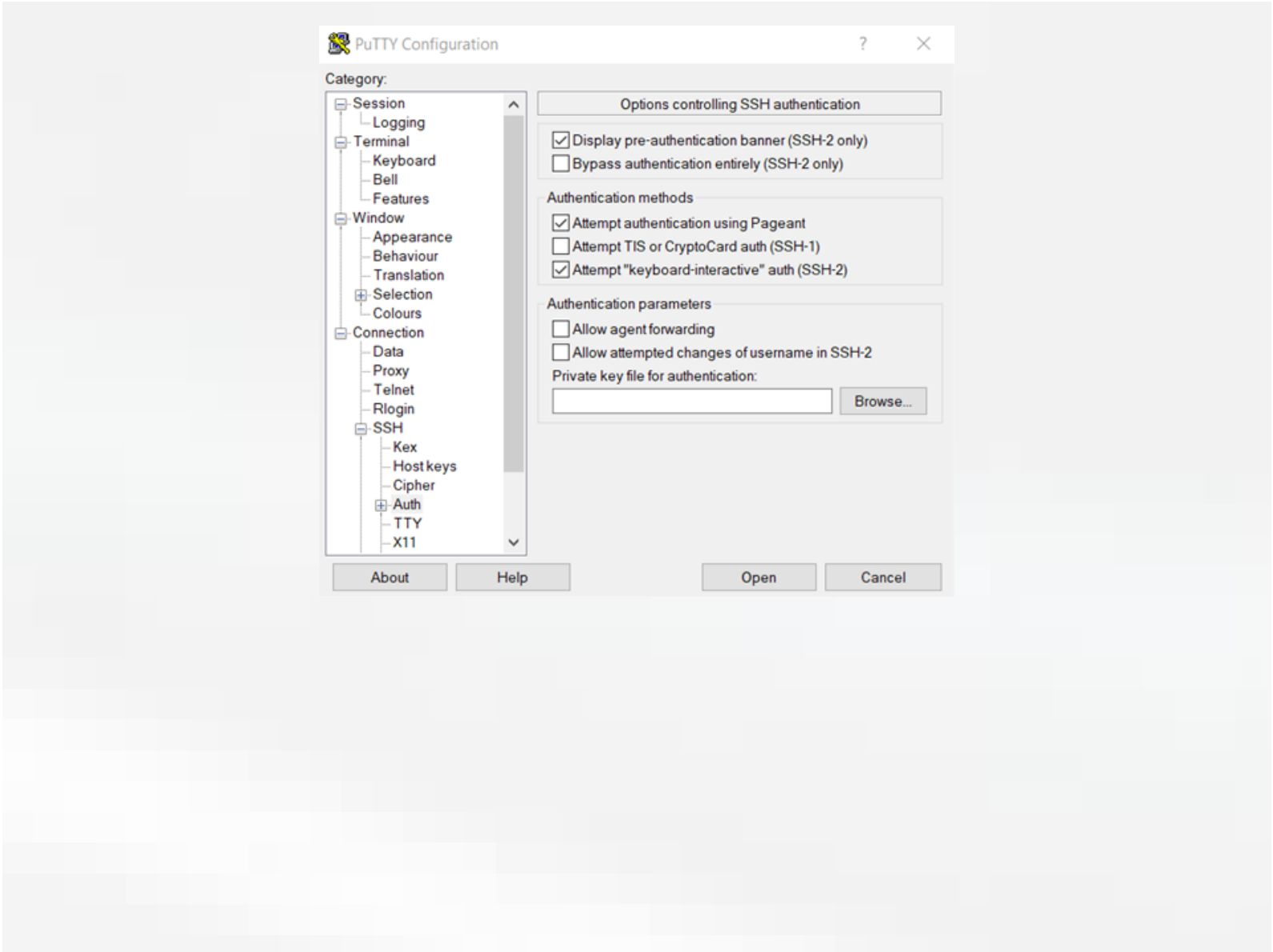

PuTTY Key Generator
File Key Conversions Help
Key
No key.
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA DSA ECDSA ED25519 SSH-1 (RSA)
Number of bits in a generated key:
2048

You should see your key as text, and need to save it. However, PuttyGen employs a non-standard format.

1. Add a passphrase (*and remember it!*)
2. Save your public and private key, using the buttons.
3. Copy-paste the key into a text editor
4. Save the text file as `id_YOURNAME.pub`. For example: `id_janjanssen.pub`.
5. Mail the `.pub` file to the trainer.

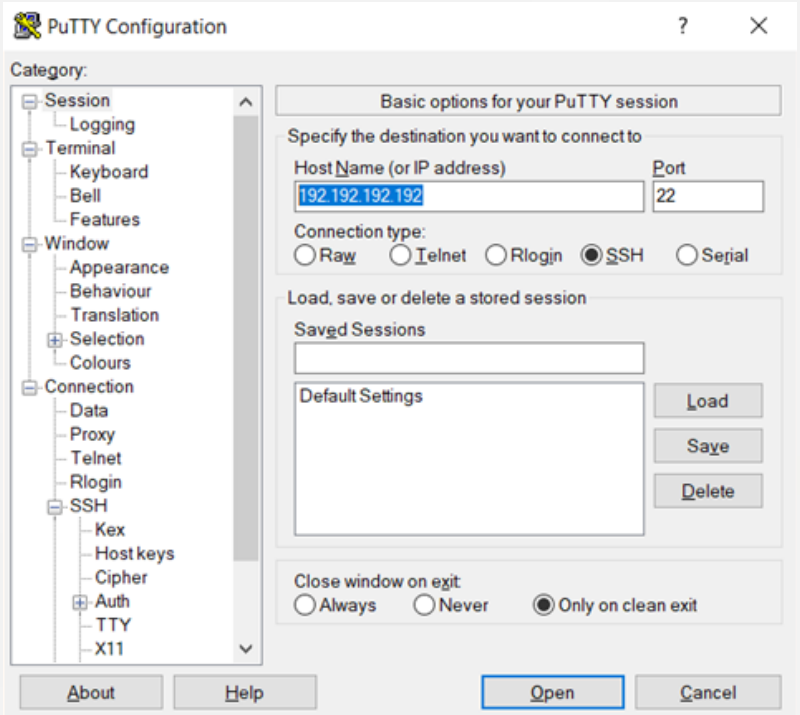
Using Putty

Open Putty and navigate to `connection/SSH/Auth`. Use `browse` to select your private key.


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Options controlling SSH authentication
Display pre-authentication banner (SSH-2 only)
Bypass authentication entirely (SSH-2 only)
Authentication methods
Attempt authentication using Pageant
Attempt TIS or CryptoCard auth (SSH-1)
Attempt "keyboard-interactive" auth (SSH-2)
Authentication parameters
Allow agent forwarding
Allow attempted changes of username in SSH-2
Private key file for authentication:
Browse...
About
Help
Open
Cancel

Using Putty

Navigate to `Session`, and fill in the IP address provided by the trainer. Finally, hit `open`.


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
192.192.192.192
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel

Using Putty

1. You should get a security alert, as your system does not know the remote system. Select `yes`.
2. Observe the terminal: this is your window to the VM
3. Use `ubuntu` as the username
4. Use your passphrase

Getting WSL

1. Open PowerShell (WIN+X, A), and run th following command:

```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Wi
```

2. Reboot when prompted.
3. After rebooting, open the Windows Store search for `Ubuntu`.
4. Click `install` or `download`, and wait for it complete.

5. When it's done, there should be an icon f
   Ubuntu. Click it, set (and remember!) you
   password.
6. Go to the next slide (down)

SSH key generation

1. In your Ubuntu terminal, type

```
sudo apt install ssh
ssh-keygen -t rsa
```

2. Follow the instructions.
3. Open the `run` dialog in Windows (WIN+R), and enter `%LocalAppData%\Packages\`
4. Find the one that has `Ubuntu` in its name

name

5. Drill down to `\LocalState\rootfs\home\`,
6. Open the folder corresponding to your Ubuntu username, and open the .ssh folder.
7. Mail the `.pub` file to the trainer.

Getting SSH (Powershell)

Type the following commands in PowerShell (type `y` when asked)

```
Find-Module Posh-SSH
Install-Module Posh-SSH
```

You now have PowerShell installed!

First, type `ssh`, and see if it still generates an error.

- If the error disappeared, you have SSH! (and you use the default `ssh` command)
- If yes, go to the next slide (down):

Using SSH (Powershell)

Create a new SSH session

```
New-SSHSession -ComputerName "YOUR_IP_HERE" -Credential (Get-
```

And follow the instructions.

Finally, run commands using

```
Invoke-SSHCommand -Index 0 -Command "whoami"
```

Note that PowerShell sends one command over SSH at a time. Replace `whoami` with the command you want to run.

Powershell SSH key generation

Start powershell, and run:

```
mkdir %userprofile%/.ssh
cd %userprofile%/.ssh
ssh-keygen -t rsa -C "your_email@example.com"
```

And follow the instructions, naming the key as follows: `id_yourname`. If this

generates an error, attract the attention of the trainer.

Open the run dialog (WIN+R), and type `%userprofile%/.ssh`. You should find two files, of which one the public (`.pub`) key. Send the public key to the trainer.

Connecting

Let's say you've mailed your public keyfile to the trainer, and he sent you the IP of your VM.

- Your `ssh key` is in `.ssh`, and is called `id_iot`.
- The IP you got is 52.59.203.96. You will then run:

```
ssh -i .ssh/id_iot ubuntu@52.59.203.96
```

  Where the -i flag stands for `identity`, and `ubuntu` is the default username.

Note that if you're using PowerShell and it's not cooperating, go to the next slide (down)

Using SSH (Powershell)

Create a new SSH session

```
New-SSHSession -ComputerName "YOUR_IP_HERE" -Credential (Get-
```

And follow the instructions.

Finally, run commands using

```
Invoke-SSHCommand -Index 0 -Command "whoami"
```

Note that PowerShell sends one command over SSH at a time. Replace `whoami` with the command you want to run.

UMP

Linux

Mac

Windows