

CS 3106 - SSH Key Generation Assignment

Abstract

Walkthrough of how to set up [SSH](#)

Content

Steps

1. Generate an SSH key pair
2. Enable SSH connection on the server
3. Upload the public key to the server to automatically authenticate on succeeding connections

Breakdown

Generate an SSH key pair



- Use the `ssh-keygen` command

Generating a keypair

```
(base) PS C:\Users\Bryan Sanchez> ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\Bryan Sanchez/.ssh/id_ed25519): D:\College\Notes\Year3_Sem1\Cybersecurity\ssh_id_ed25519
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in D:\College\Notes\Year3_Sem1\Cybersecurity\ssh_id_ed25519
Your public key has been saved in D:\College\Notes\Year3_Sem1\Cybersecurity\ssh_id_ed25519.pub
The key fingerprint is:
[REDACTED]
The key's randomart image is:
[REDACTED]
```

- Parameters
 1. Path (optional) - Path to file where key is saved (if not provided, it will save it in the path it specified)
 2. Passphrase (optional) - passphrase used to safeguard keypair (prevents malicious attackers from gaining access to them if they breach your device)
- This will generate a public private key pair (`PUB` file is the public key)

Generated Files

 ssh_id_ed25519	11/22/2024 9:19 AM	File	1 KB
 ssh_id_ed25519	11/22/2024 9:19 AM	PUB File	1 KB

Custom Path

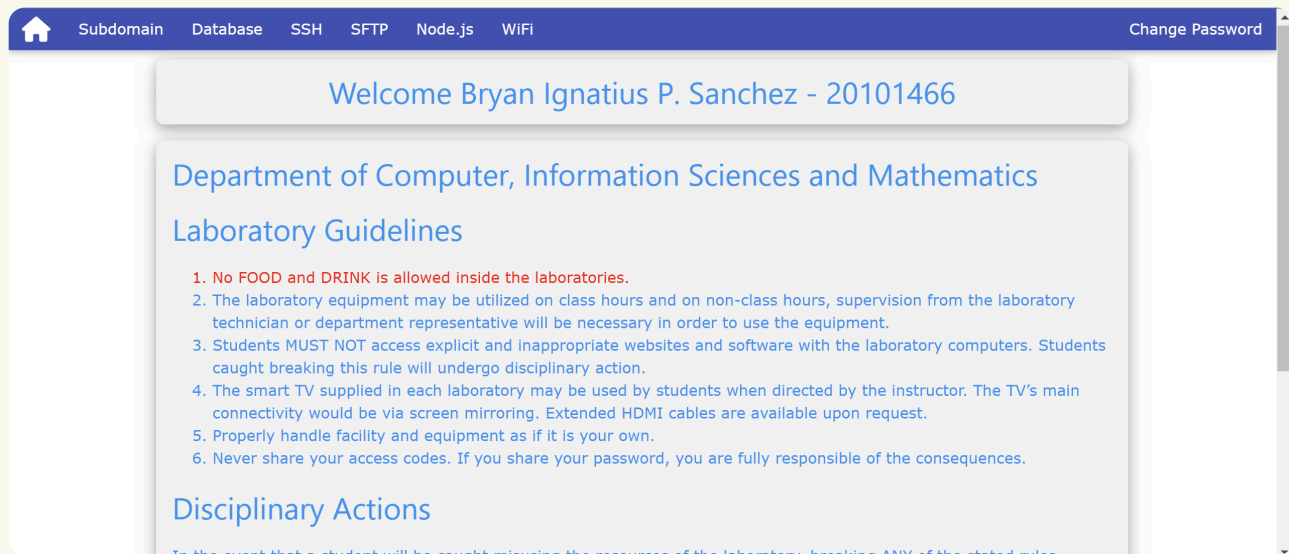
If you use a custom path, when connecting via SSH later, add the `-i` flag to specify the path to the private key since, by default, SSH will look for it in the default path specified by the `ssh-keygen` command.

```
ssh -i path/to/private_key_file ...
```

Enable SSH connection on the server

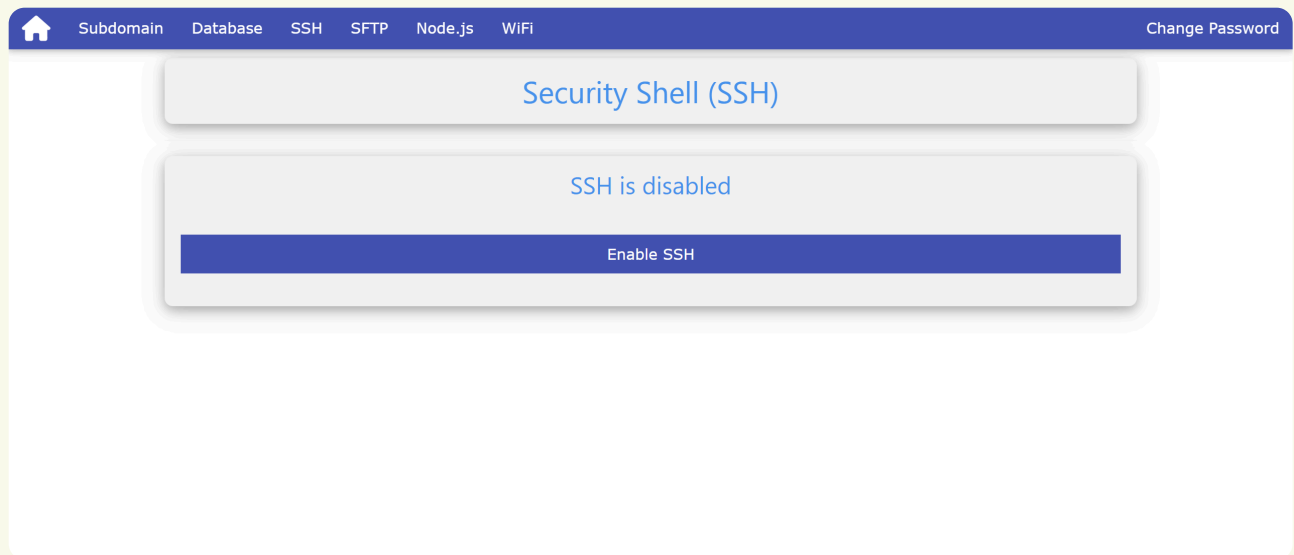
- Go to admin.dcism.org and log in

Homepage after logging in



- Go to the [SSH](#) tab and click [Enable SSH](#)

Enabling SSH




Upload the public key to the server to automatically authenticate on succeeding connections

- Upon enabling SSH, use the command provided to connect to the web server via SSH

Viewing the SSH command

SSH is enabled

 Username: **s20101466**
Server: **web.dcism.org**
Port: **22077**
Command: **ssh -p22077 s20101466@web.dcism.org**

Disable SSH

- Enter the command in your terminal
 - You will be prompted to enter your password

Using the SSH command

```
(base) PS C:\Users\Bryan Sanchez> ssh -p 22077 s20101466@web.dcism.org
The authenticity of host '[web.dcism.org]:22077 ([203.96.181.254]:22077)' can't be established.
ED25519 key fingerprint is SHA256:qTw5lr2mVff04IS66mIw3m4GoI6IjE01Uo7EWyYd7MA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[web.dcism.org]:22077' (ED25519) to the list of known hosts.
s20101466@web.dcism.org's password:
```

- Upon successful connection, create a `.ssh` folder in the root directory (i.e. `~/ .ssh`) to upload the public key into

Creating a `.ssh` directory

```
s20101466@web:~$ mkdir .ssh
s20101466@web:~$ cd .ssh
s20101466@web:~/ .ssh$ |
```

- Create a file called `authorized_keys` via `nano authorized_keys` and copy-paste the contents of the generated `PUB` file from step 1 into `authorized_keys`

- Upon saving the file, log out of the SSH session and reconnect, specifying the private key you generated earlier. Doing so should allow you to log in w/o needing to specify a password

References