

## Technical Skills

Awesome project - [Report](#) with [video](#)

This is a complete end to end search, planning, implementation and execution of an attack as a hacker with a spyware I created for this project. It demonstrates my technical skill as listed below to carry out an viable and potentially impactful attack on a targeted user. I also acquired additional skills such as the way to use AWS services including API Gateway, Lambda function and Dynamodb. Please find details and evidence of my achievement in the report and video. The source code was only shared with my tutor for marking purposes.

- History and categories of computer viruses
- Creation of a spyware which does keylogging and send it to my AWS service
- Importance of having anti-virus software (because my spyware could be caught by one and I take it as a compliment)
- Email phishing in both the project and [weekly activity](#)
- Email From spoofing
- Disguise executable files as images
- Exploit security through obscurity of Powershell
- Hide traces of the spyware and make it self executing at system boot
- Generating and of AWS AMI keys and tested with Postman

## SQL injection

While doing Comp6441, I did all 3 levels of extended activity 01. [Blog](#).

## Codes

I wrote code for weekly activities which helped me come up with the solution. They are 100% original which reflects my technical skills.

- One time Pad [Blog](#).
- Login leaks [Blog](#)

## RSA

During class discussion of the study case, I explained the application of public and Private key to my group which generated a visual artifact of how it works. It was covered in this [blog post](#). Eventually the course covered the detail of RSA, which I recorded in my [reflection](#).

## Bits of work

I explained with another class member in front of the class during the tutorial about how to calculate an answer for a weekly activity task [bits of penguin](#) early in the term. I briefly mentioned about it in my reflection [blog post](#).

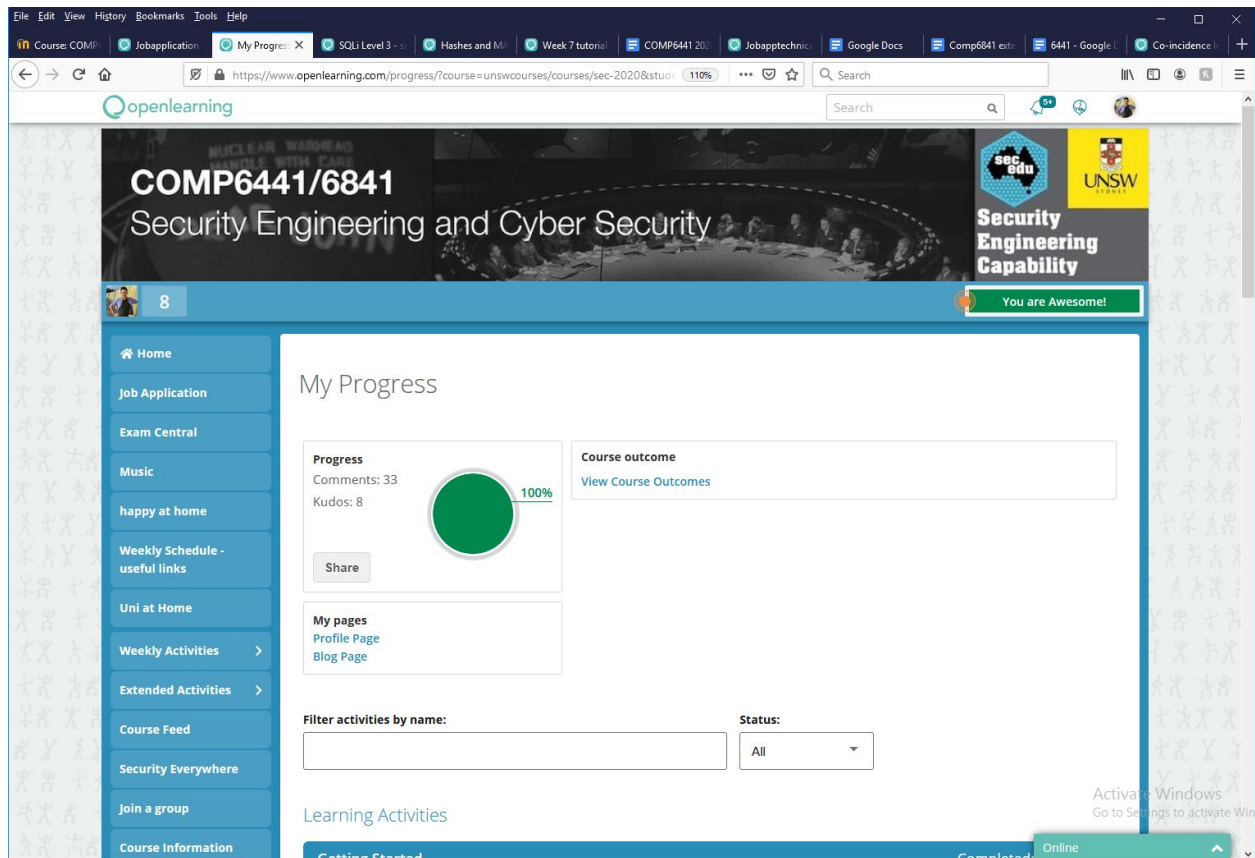
Co-incident index

I was the first coming up with an answer during an tutorial activity as recorded in my comment in the screenshot recorded in my [blog post](#).

Threat Modeling

I created a diagram for analysis of a weekly activity. [Blog](#)

Completion of all weekly activities:



Technical skills acquired during weekly activities with no additional blog or work log as proof:

HMAC

Modes of AES

## Encryption and Decryption of Ciphers

### Symmetric Ciphers

#### Substitution cipher

#### Transposition Cipher