Project Portfolio

Week 1

-Sorting which project team im in

Week 2

- Re-Learning to use ZAP

We had slightly touched on using ZAP during the Security paper which I had taken last semester, though I had forgotten simple set up protocols so had Faisal send me an old lab from the security paper which helped me do so. I installed Kali Linux using Oracle VM, James showed me how to do this as I got slightly stuck on a couple of steps. Once Kali Linux was installed, Faisal suggested that I use pen testing to practise my security vulnerability scanning skills using ZAP. I used the following link to help me get the pen testing server up and running using oracle VM. <https://www.explainhownow.com/2019/learn-penetration-testing/>.

- Installing Kali Linux

- Using a browser as a proxy to automate zap checks

-Downloading Pentester image to use pentesting examples

Week 3

Getting the pen testing server running took me longer than it should have, I ended up using the first lesson of week 3 to figure this out. In the end the solution was simple I just had to download the pen testing image from the website and use it to run the server I created on Oracle VM. Once on the server I use the ipconfig command to check for I.P and use the I.P as the link in any browser to connect to the server. Working through the pen testing examples was interesting and refreshed my memory especially with the SQL injections. I realised that ZAP was not 100% effective in scanning for vulnerabilities for the pen testing examples, this tells me that having your own knowledge or running extra vulnerability scanners is important to have higher efficiency in finding and fixing vulnerabilities. Faisal suggested that I use a browser to act as a proxy so I could automate my vulnerability scans for any webpages I visited. The process in doing this seemed relatively simple while getting help from Faisal and using tutorials to help me do so. Although after following all of the steps I failed to get feedback from ZAP using the browser proxy. This is something I will have to research further.

-Getting stuck using a browser as a proxy

-Pentesting using Zap

Week 4

I worked through most of the pen testing examples and managed to find vulnerabilities for most. I heard about another tool called Nessus which is mostly used for networking vulnerability scanning but has modules to scan web applications also. I decided to give it a go and installed this on my Kali Linux machine so I could compare vulnerability results to ZAP. Nessus was relatively straight forward to set up using a tutorial along the way. The initial scan I did took much longer than a scan on ZAP and produced much more results, which were mostly network vulnerabilities. During class Corey (2nd semester project student) guided me through basic gitlab services which students or lecturers may ask me. The documentation the various different protocols was good so I felt I could learn how to do this if need be. We concluded the session by having a quick meeting with the group to explain what we were all doing and to ask any questions if needed.

-Learnt some basic about gitlab

-Add users

-Create new projects/repositories

-Lesson 2 - Meeting with Faisal- Sort out what direction we are all going in

Week 5

We had a meeting which we were all to give a 3minute explanation on what tasks we were all working on. I found it hard to explain the different tasks I was working on especially when it came to working with a tool called Selenium. I have been watching tutorials on how to set up Selenium but to no avail as of yet. I will continue to progress on Selenium until I set this up because Faisal told me this was an important tool and could be important in future job roles.

-Lesson 1 meeting with Faisal – 3min talk on what were all doing.

-Trying to learn Selenium