Reverse Engineering week3

What I did

Install or download tool for inverse assembly.

First one is objdump.

Really famous for Linux but seems really limited for utility and

cannot understand how to patch binary using this.

For ease to use, just confirm binary file maybe useful.

Second one Ghidra (from NSA).

I was stacked when I export program file because Ghidra seems export file as

.bin file. So, I couldn’t but later I just implement the file from terminal and

that’s worked !!

I’m thinking should use this tool for this project or not maybe ask tutor !!!.

Better to remember instruction

Something Awesome

Goal:

Be familiar with Reverse engineering (Binary), get skill to solve immediate easy Crackme or CTF quiz.

Background:

For Programming, we normally use high level language like Python, Java, C, the reason why uses these language is these high level language is easily readable for human. On the other hand, Computer can only read binary words, so we need convert our language to binary words (compile). But binary words are too difficult for human to read so we make assembly language(basic) for human reading.   
In security, it is really important to understand these assembly language and trace what computer did for job since if these binary text change, their works also change.

Therefore, study reverse engineering would be one of the most important topic for security and it is really interesting to trace computers work by reading assembly and binary language(like talking with computer !!)

So far what I did is install Reverse engineering tools (objdump, Ghidra) and attempt

some easy quiz (from <https://reverse.put.as/crackmes/>)  
Pass:

- Be familiar with Reverse engineering (write blog for each week about technology)

Credit:

- Complete the above

- Solve some easy questions (Crackme, CTF)

Distinction:

- Complete the above

- Solve immediate level questions

High Distinction:

- Complete the above

- Do extra things using Reverse Engineering tool (like report

Time Management:

Week1: find something awesome project

Week2: Study about Reverse Engineering and Make Environment for this

Week3: Keep Study and try some easy Crackme question or enjoy playing but not for illegal things!!

Week4: Keep Study and easy quiz but try more quizzes and study about more Ghidra

Week5: Keep above but try immediate quiz as well

Week6 ~ Week10: Keep doing above but can change flexibly.

Using OAuth.

It is really famous making phishing worm using Google OAuth system.

(For example, in this case just send email to her with some attracting sentence to let her open button with google masquerading logo, then attacker would get her email account.) In this system, Google authenticate users instead of resource owner (company) to give permission for web applications or log in website. In my opinion, the reason why people easily deceived by this trick is for high trust of Google. People normally think that this website and web application is truthful because of Google authentication. However, it is better to keep in our mind that evil guys can trick people by using this common sense.

referring website: <https://arstechnica.com/information-technology/2017/05/dont-trust-oauth-why-the-google-docs-worm-was-so-convincing/>