Please read the attached document on Facebook quiz’s and summarize the important points in 2/3 pages. This lab is to be completed in pairs and should be uploaded before Sunday 9th March.  
  
  
  
About introduction:

Social engineering can take many forms from technology based like email spam, pop-up windows, phishing web sites to in person techniques: pretexting, phone phishing. They can be obvious (or not) depending from the level of awareness of the targets and the skills of an attacker. Presented in introduction quiz ‘**What does your password say about you?**’ is an example of online tool for easy gathering of password information. Study of four presented questions suggests that there is not much work left for guessing right combination of characters. It is worth to point out that questions in this quiz (and similar) target specific sensitive data so the level of awareness of the quiz-taker who honestly answered them must be very low. Author of the text calls the quiz “harmless at first glance”, it is hard to believe how somebody could not be conscious of the purpose of it.

A little bit of history:

As the term social engineering has become popular with the development of the technologies, we must mention that it was invented and used long time before anyone even thought about online quiz game. Author of Which Disney© Princess are YOU quotes story of Isaac from The Old Testament and the Trojan horse of the Greeks from the ancient times to nowadays portraits of Frank Abaganale or Kevin Mitnick. Aside of people trying to deceit other, nature gives us examples of social engineering among flora and fauna. Chameleon changing skin hue, flowers emitting scent.

Today’s opportunities:

When it comes to social engineering there is always about the information that can be used:

* Intellectual properties
* Exploitable vulnerabilities
* Emails, passwords, logins
* Personal details, credit card numbers.

As technology develops different ways of communication, new methods arise for attackers to use them. It also provides environment for safer way of getting the information than if it was physical attempt to obtain information. Today’s social engineering has wide range of tools to use like social networking sites, email services, p2p networks. Often users give a lot of details themselves without knowing who exactly and how will use those information i.e. Facebook account holders give personal details just by assigning to the service. Facebook gives a lot of room for maneuver for information hunters by providing wide access to application developers (quiz and other information gathering authors).

Quiz results:

Researches carried out on five Facebook users (each one took a part in set of prepared quizzes) resulted in profiles made individually for each person. Allowing for quiz to access profile details gathered most basic information: name and email address. Incidentally speaking it is curious what would be the time span before these addresses get malicious email content. Further results compilation shows how seemingly harmless sets of questions-answers allow for developing precisely targeted attack. It can be aimed on quiz victims (phishing email, in person pretexting) as well as third party institutions like banks.