SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1 2014

Tutorial questions for Lecture 2: Threats, Vulnerabilities and Attacks

*Attempt these questions **before** you attend your session, and bring your prepared answers with you. Come prepared to discuss your answers and/or any problems you encountered in trying to answer these questions.*

QUESTION 1

Clearly explain:

a) The difference between vulnerabilities and threats. Give an example to illustrate your answer.
b) The relationship between threats, vulnerabilities and attacks.
c) Is it possible for a threat and a vulnerability to coincide without an attack occurring? Explain your answer.
d) The difference between passive and active attacks. Give an example to illustrate your answer.

QUESTION 2

Your current position as a QUT student requires you to access and use information assets, and to develop your own information assets. This question concerns the information security of your personal information system with respect to your PC or mobile device.

a) Identify threats to the information assets you have developed and stored. Make **two** lists of possible threats: one for those related to natural events, and one for those related to human actions. Include at least four threats on each list.
b) For each identified threat, determine which security goal is affected.
c) Identify vulnerabilities associated with the scenario above. Try to list at least **five** vulnerabilities.
d) Considering the threats you listed and the vulnerabilities you have identified, are there any plausible attacks on your information assets?

QUESTION 3

Visit the AusCERT website http://www.auscert.org.au/. Follow the links to the Security Bulletins page, and use the information from this site to answer the following questions:

a) What sort of information is included in the security bulletin titles (Look for AusCERT Bulletin Format)?
b) What information is conveyed in the security bulletin *title* for the security bulletin numbered ESB-2014.0230?
c) Read the bulletin. Describe:
    i. the vulnerabilities.
    ii. what could happen if these vulnerabilities are exploited.
d) Does an attacker need the user to take any particular action in order to exploit these vulnerabilities?
e) How can this problem be prevented?

QUESTION 4

To protect information assets you need to know what your assets are, and where they are stored. However, many organizations overlook data storage in devices such as photocopiers and printers. Read the CBS News article "Digital Photocopiers loaded with secrets" available at:

http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml

With this in mind, answer the following questions:

a) Suppose an organization sells their used photocopier at auction without first removing the stored data from the hard drive. Which information security goal will potentially be breached if this data is exposed?
b) Is disposing of the used photocopier considered a threat, vulnerability or an attack? Explain your answer.
c) Many photocopiers are multifunctional and also operate as printers for other networked devices. Describe a threat to information assets that may arise through the use of these devices within the organization (that is, before they are decommissioned).
d) Visit the AusCERT website and look at Security Bulletins listed under the category

‘Dedicated Device’. Some bulletins related to printers. View some of these to find out what attackers can do, and the type of access they need to enable these actions.

QUESTION 5

The article ‘*Trojan program hijacks World of Warcraft accounts despite two-factor authentication*’ available at:

http://news.techworld.com/security/3495965/trojan-program-hijacks-world-of-warcraft-accounts-despite-two-factor-authentication/

describes the situation where players’ computers became infected with malicious code. Answer the following questions based on the information contained in the article.

a) Why is the malware described as a Trojan?
b) What is the legitimate function performed by the downloaded software?
c) What is the additional function performed by the software, without the user’s consent?

QUESTION 6

Consider the following scenario: An employee finds a portable storage device (a USB) in the foyer of the company office building. The employee thinks that the USB was most likely dropped by another employee, and decides to access the contents on the device in an attempt to discover the device owner and return the lost property.

a) Outline likely threats associate with this scenario.
b) What sort of vulnerabilities may exist within the organization?
c) Suppose the USB contains malicious code which infects the organization computer system. Given that the employee did not intentionally introduce the viral code, would this be considered an attack? Justify your answer.