TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI

VICTORIA
UNIVERSITY OF WELLINGTON

EXAMINATIONS – 2012

TRIMESTER 2

NWEN 405

Security Engineering

Time Allowed: 2 Hours

Instructions: *Read each question carefully before attempting it.*

This examination will be marked out of **100** marks.

Plan on spending about 1 minutes per mark.

Answer **ALL** questions.

You may answer the questions in any order. Make sure you clearly identify the question you are answering.

Only printed foreign/English dictionaries are permitted.

You are permitted one double-sided TYPED A4 page of notes.

Question	Topic	Marks
1	Secure Software Engineering Techniques	23 marks
2	Malware, Anti-Virus and Worms	8 marks
3	Web Applications	24 marks
4	Network Security	25 marks
5	Firewalls and IDS	20 marks

Question 1. Secure Software Engineering Techniques [23 marks]

(a) [5 marks] Identify TWO data specific threats using the Microsoft STRIDE methodology and give an example of each of these threats in the context of a student records database.

(b) [5 marks] Why is it not safe to assume that a hard-to-find bug is of low risk to a system? Justify your answer.

(c) [5 marks] Consider a software application *A* that is estimated as having 90% fewer bugs after testing than it had before testing. Explain why we can say that the application is now more reliable but not necessarily more secure.

(d) [5 marks] Do you agree with the assertion "All software vulnerabilities identified by static analysis tools are really vulnerabilities"? Briefly justify your answer.

(e) [3 marks] Define how *risk* can be calculated in terms of probability and damage potential.

Question 2. Malware, Anti-virus and Worms [8 marks]

(a) [3 marks] Briefly explain the key differences between *independent* and *parasitic* malware.

(b) [5 marks] Define the term *fast scanning* in the context of a *warhol worm* and explain its advantage over previous similar techniques.

Question 3. Web Applications [24 marks]

(a) [5 marks] Outline an attack on a web application that sends authorative state (for example, the cost of a pizza) as a hidden field from the client application to the server. Explain why your attack would work.

(b) [4 marks] Define the *same-origin policy* used by browsers.

(c) [5 marks] Outline an *XSRF* attack that could occur if the following conditions existed. A user who has authenticated themselves to `myvuw.ac.nz`, done a transaction and closed the window. Without closing the browser, they visit my site `allyourbasebleongtous.com`.

(d) [5 marks] Describe a way to defend against *XSRF* attacks.

(e) [5 marks] Briefly outline how a scenario for a *XSS* attack.

Question 4. Network Security [25 marks]

(a) [5 marks] Outline a *TCP SYN flooding* attack.

(b) [5 marks] Successful execution of a *TCP Session Hijack* attack requires guessing the correct sequence number expected by the server. List TWO ways to determine the correct sequence number to use.

(c) [5 marks] Briefly describe TWO fixes introduced in an attempt to prevent Kaminsky's attack on DNS servers succeeding.

(d) [5 marks] Draw a botnet that uses a *distributed C&C structure* and clearly identify the role of each component in the structure.

(e) [5 marks] Outline how a *dead drop* could be implemented for botnet communication.

Question 5. Firewalls and IDS [20 marks]

(a) [10 marks] Describe the similarities and differences between the following types of firewall: packet filter; stateful packet filters; application-layer firewalls; and, personal firewalls.

For each, be sure to consider: (i) at which level in the network stack that each operates; (ii) what criteria it can apply when deciding whether to block or allow traffic.

Organise your answer in the form of a table.

(b) [10 marks] Consider misuse/signature-detection and anomaly-detection network intrusion detection systems (IDSs).

Compare these two IDSes in terms of: (i) False positive rates; (ii) False negative rates; (iii) Ability to determine the type of attack; (iv) Accuracy in rapidly changing environments; (v) Performance over time.

Organise your answer in the form of a table.

****