

UNIVERSITY OF BOLTON

**SCHOOL OF BUSINESS AND CREATIVE
TECHNOLOGIES**

**MSC INFORMATION TECHNOLOGY SYSTEMS
DEVELOPMENT**

SEMESTER 2 EXAMINATIONS 2009/2010

INTERNET SECURITY

MODULE NO: MIT4103

Date: **Friday 4 June 2010**

Time: **10.00 am – 12.00 pm**

INSTRUCTIONS TO CANDIDATES:

There are **SIX** questions on this paper.

Answer ANY FOUR questions.

All questions carry equal marks.

QUESTION 1

This question makes reference to the Scenario available for students to study in advance of the examination a copy of which is to be found at the end of the question paper.

- 1a Explain briefly with the aid of a diagram the relationship between Assets, Vulnerabilities, Threats and Impacts in terms of their contribution to an assessment of risk in the context of computer security. (4 marks)
- 1b Assuming the companies competitors are gaining information without help from anyone within or physical entering ElectroMetro, what do you consider to be the most likely ways in which information about the bids the company is preparing could be accessed? Justify your answers with a brief explanation of how each attack would operate. (14 marks)
- 1c Identify the assets in the Scenario which are specific to the company and might be targeted by a hacker employed by a competitor. Consider what value you would place on these assets and explain what you have taken into account when arriving at a valuation. (7 marks)

QUESTION 2

This question makes reference to the Scenario available for students to study in advance of the examination a copy of which is to be found at the end of the question paper

- 2a Outline the difference between Packet Filtering Firewalls and Application-proxy Gateway Firewalls in terms of the layer of the 7 layer OSI model they operate at and the criteria typically used to filter at each layer. (9 marks)
- 2b Given that the PIX firewall operated by ElectroMetro applies Source Network Address Translation (SNAT) explain using a diagram how SNAT operates for internal clients accessing a Website on the Internet. Show typical packet header data and indicate clearly the changes made by the firewall to packets leaving and entering the companies Internal network. (10 marks)
- 2c Explain why the firewall needs a NAT table and how the table is used. (6 marks)

Please turn the page

Business and Creative Technologies
MSc Information Technology Systems Development
Semester 2 Examinations 2009/2010
Internet Security
Module no: MIT4103

QUESTION 3

This question makes reference to the Scenario available for students to study in advance of the examination a copy of which is to be found at the end of the question paper.

3a In the ElectroMetro Scenario the company wants to provide secure access to the Accounts server for the companies accountants. Suggest how this should be achieved and discuss briefly the security implications of your solution.
(7 marks)

3b With reference to the recent TJX intrusion and associated court cases, discuss the increasing professionalism of Internet-based attacks, the implications this has for Internet security, and the potential impact of the Payment Card Industry-Data Security Standard.
(18 marks)

QUESTION 4

4a Outline the concept of the 'porous perimeter' explaining why a perimeter firewall is no longer regarded as adequate security for corporate networks. You should identify specific technological advances and changes in working practices that gave rise to this concept.
(9 marks)

4b The concept of layered security has evolved largely to combat the disappearance of a well-defined perimeter. Sketch a diagram to illustrate this concept showing typical security hardware and software employed then explain how it would typically facilitate the detection of, and reduce the potential impact of, malware which infected a server on the internal network.
(16 marks)

QUESTION 5

5a Phishing attacks are one of the most prominent category of attacks currently affecting Internet users. Explain how the various elements associated with this activity fit together and which human emotions are targeted providing typical examples to support your answer.
(18 marks)

5b Why it is proving to be very difficult to eliminate phishing attacks?
(7 marks)

Please turn the page

Business and Creative Technologies
MSc Information Technology Systems Development
Semester 2 Examinations 2009/2010
Internet Security
Module no: MIT4103

QUESTION 6

6a Network scanning is a technique widely used both by hackers and malware. Discuss why it is used, how it operates, and how such attacks can be hidden from signature-based Intrusion Detection System. Finally explain a technique which can be used to significantly slow down network scans.

(14 marks)

6b Despite the defenses provided by layered security computer viruses and worms still affect a large number of corporate networks each year. Explain why it is that the defenses are so ineffective and discuss recent developments to address this problem.

(11 marks)

END OF QUESTIONS

Please turn the page

Business and Creative Technologies
MSc Information Technology Systems Development
Semester 2 Examinations 2009/2010
Internet Security
Module no: MIT4103

INTERNET SECURITY SCENARIO

ElectroMetro produces electric tram systems which are operational in several cities around the world. A typical contract would be between £50-100M and take several years to design, build, install and commission. The company is currently coming to the end of its last contract with design and build completed. They have competed unsuccessfully for three large contracts only to find that they have been undercut by the same French competitor who seems to have inside knowledge about their bids. Another bid is being prepared for 16th March 2009 worth in the region of £70M which would guarantee work for the company for another four to five years, however if this fails it is feared that large scale redundancies would be unavoidable.

The company employs around 270 staff about 80 of whom work in the fabricating shed and 150 of which work in the offices. The remaining staff are drivers, security, and estates workers many of which are part-time. Physical security is relatively tight with high perimeter fencing, CCTV and card operated barriers on the entrances. Visitors are required to report to the gatehouse where they are issued with temporary passes and have to sign in to the visitor's book. Cleaning is carried out by a local company and catering is done on contract by a well-known catering corporation.

As with many long-established heavy engineering companies the computing facilities in the Fabricating Shed are fairly primitive consisting of around twenty XP workstations that were modernized in 2005 to use wireless ethernet. Desktop computers in the main offices are connected using switched ethernet. The office building has a 10Mbps Broadband Internet connection through a Cisco 3620 router and a Cisco PIX 515 firewall. The company has a static Website running Apache as an application on a virtual linux server. This and the server for the companies Computer Aided Drawing software both run on the same virtual host along with the DNS server and one of the companies Active Directory Domain Controllers. A second virtual host runs the companies other Active Directory Domain Controller along with the Accounting software and Payroll system. Email including Webmail is provided using Microsoft's Exchange server running on a dedicated Dell server. Computers are mainly Dell workstations although a number of the sales staff and senior engineers and management use laptops which they connect using WEP encryption to a Cisco wireless access point on each floor of the offices.

According to local sources the company suffered badly from strike action in the late 1970's after which the consortium cut investment and shed nearly three hundred jobs causing severe hardship for the former workers many of whom never found subsequent employment. The company has never enjoyed a good relationship either with the local townspeople or with the local press, a situation which has not improved with the recent disclosure that a high proportion of workers in the fabrication shed are of Polish origin.