

UNIVERSITY OF BOLTON

**SCHOOL OF BUSINESS AND CREATIVE
TECHNOLOGIES**

COMPUTING PATHWAYS

SEMESTER 1 EXAMINATIONS 2009/2010

INTERNET SECURITY

MODULE NO: CST3104

Date: Friday 22nd January 2010

Time: 10.00 – 12.00

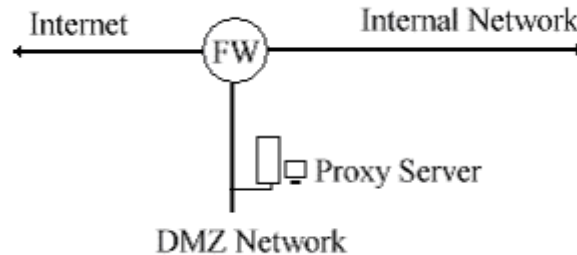
INSTRUCTIONS TO CANDIDATES:

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

Answer **ANY FOUR** questions.

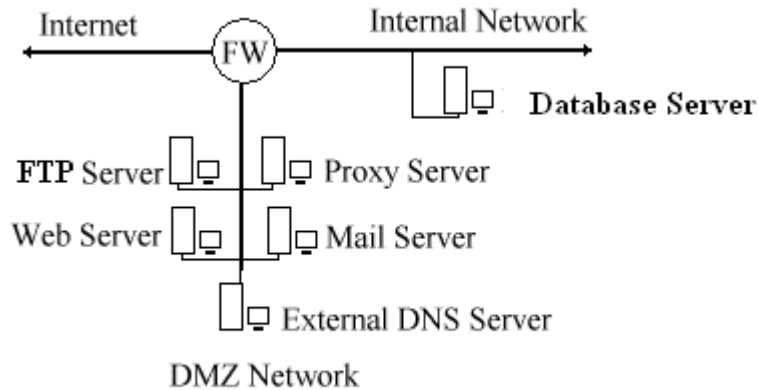
All questions carry equal marks.

QUESTION 1



- 1a/ In the above diagram the DMZ network has address 172.17.20.0/24 and the Internal network has the address 192.168.40.0/24. The address of the firewall's external interface is 193.63.48.31. Assume the addressing of the firewall's other interfaces follows the normal convention. PAT (SNAT) is applied to traffic between the Internal network and the Internet. A network analyzer is monitoring all the interfaces on firewall FW. What would be the source and destination IP addresses and port numbers of all packets associated with the TCP/IP 3-way handshake starting a connection from a browser on host 192.168.40.100 on the Internal network to an http server with address 149.170.191.253 on the Internet. (You should chose representative values for the client source port numbers.)
 (11 marks)
- 1b/ Another client on the internal network with IP address 192.168.40.27 starts a TCP connection with the http server at 149.170.191.253 on the Internet whilst the connection detailed in 1a/ above is still open. Explain how the Firewall manages to direct the return packets to the correct internal client.
 (7 marks)
- 1c/ After a few months the response time for the Internet early in the morning becomes poor and a check of the firewall log reveals many internal clients are accessing the same websites to read work-related material. Consequently a proxy server is introduced into the DMZ as shown in the diagram above. What configuration changes would be needed on the firewall and internal clients to bring the proxy server into operation and prevent internal clients from bypassing the proxy server?
 (7 marks)

QUESTION 2



2a/ In the above diagram the DMZ network has address 172.17.20.0/24 and the Internal network has the address 192.168.40.0/24. The address of the firewall's external interface is 193.63.48.31. The Web Server in the DMZ on 172.17.20.2 is accessible to clients on the Internet through the use of Port Forwarding (DNAT). There is no requirement for NAT between the Database server 192.168.40.250 on the internal network and the DMZ. Create a table in which you show the source and destination IP addresses and server port numbers for all TCP/IP 3-way handshake packets associated with an http request for a dynamically created Webpage containing data from the database. The request comes from a firewall with IP address 149.170.191.253 on the Internet and the packets should be shown in the order they would arrive at the firewall.

(14 marks)

2b/ Last year (2009) saw the demise of several large botnets. Discuss why this happened with reference to the way Botnets operate, and what impact it will have on the Internet security scene.

(11 marks)

Business and Creative Technologies

Computing Pathway

Semester 1 Examination 2009/10

INTERNET SECURITY

Module No. CST3104

QUESTION 3

3a/ Assume you have been given the task of hardening a Web server in the DMZ against attacks from the Internet. You should assume that you have no knowledge of the software/scripts which run on the server and that responsibility for these lies with the head of the development team. Outline the types of attack you would address and discuss the ways in which you would attempt to prevent or mitigate them. You should provide a brief technical explanation of how the techniques you would employ actually work. Finally comment on the likely effectiveness of the measures you would put in place justifying your comments by reference to the known limitations of these techniques.

(25 marks)

QUESTION 4

4a/ One of the most effective forms of attack used against the software on Internet-connected servers is the Buffer Overflow attack. Explain how this attack works, what it can achieve and why new opportunities to exploit it arise.

(10 marks)

4b/ Self-encryption with a random key is a technique used by many forms of malware. Why and how is it used?

(5 marks)

4c/ A recent Webinar by a leading security vendor claimed that existing signature-based antivirus software was becoming ineffective. Outline his argument then discuss how the widespread use of cloud computing might lead to more effective defence against malware than is currently possible.

(10 marks)

PLEASE TURN THE PAGE

Business and Creative Technologies
Computing Pathway
Semester 1 Examination 2009/10
INTERNET SECURITY
Module No. CST3104

QUESTION 5

5a/ 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)

5b/ As a manager of a small network you are asked to provide a VPN to allow the companies accountants to securely access the accounts server on the internal network. Outline the different ways in which this could be achieved and the relative advantages and disadvantages of each before selecting the one which you consider to be most suitable in this case. Briefly justify your decision.

(11 marks)

QUESTION 6

6a/ Outline the concept of the porous perimeter in the context of network security then explain why a layered approach to security is used to address this problem. Use examples to support your explanation.

(10 marks)

6b/ Discuss the security challenges that arise from the widespread adoption of server virtualization within the enterprise.

(15 marks)

END OF QUESTIONS