Network Security and Cryptography

SAMPLE TIME CONSTRAINED ASSESSMENT

Answer ALL questions.

Clearly cross out surplus answers.

Time: 4 hours

The maximum mark for this paper is 100.

Any reference material brought into the examination room must be handed to the invigilator before the start of the examination.

Answer ALL questions

Introduction

Paramount Finance UK Ltd is a financial service company that provides wealth management, insurance, and investment-related services to customers primarily in the United Kingdom. The company's headquarters is based in London with branches in Manchester and Leeds. The company hosts a public web server and email server located at its main headquarters and private file servers located at all sites which are used to host and share sensitive files and data between employees and clients.
The current network architecture of Paramount Finance UK Limited is shown in **Figure 1** below.

Details of the task

Each question outlines specific scenarios faced by your client, Paramount Finance UK Ltd. You are tasked with devising security strategies for them, providing technical advice and implementations to enhance the security of the company's core network infrastructure.
Your proposed solution needs to be both technical and specific especially in terms of what tools/ software/ resources/ techniques/ configurations you recommend.

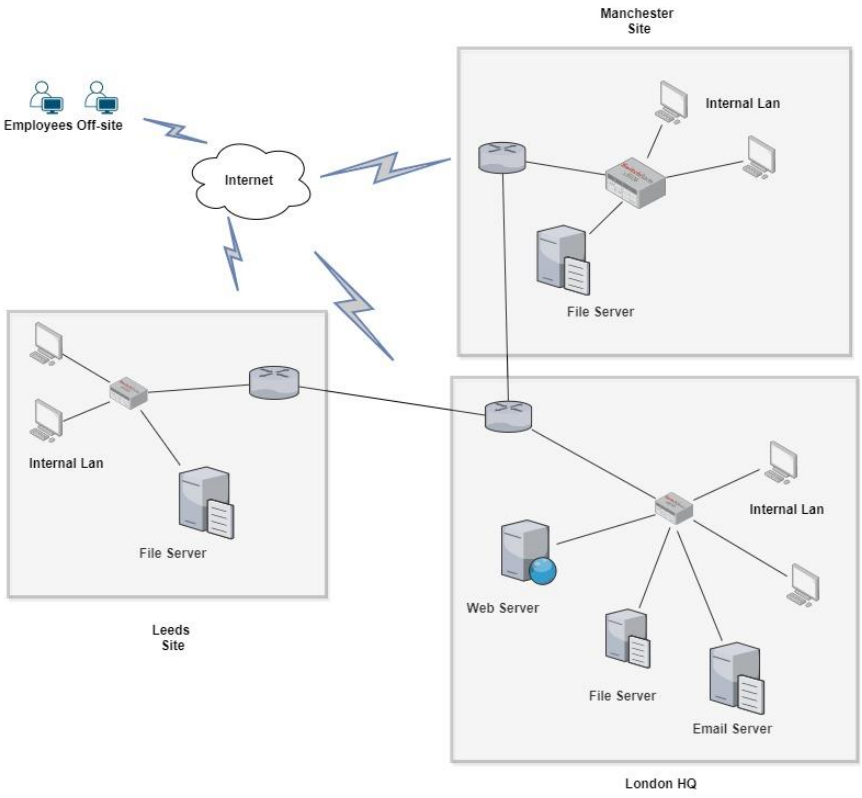

Figure 1. Paramount Finance UK Ltd.'s Network Architecture

© NCC Education Limited 2021

Question 1 – 25 Marks

Some employees work off-site but can access their workstations via remote access directly using Remote Desktop Protocol (RDP). However, exposing RDP to external users over the internet is thought to put the corporate network at risk due to known vulnerabilities.

a) Describe in detail good practices (including appropriate protocols) and recommendations you will implement to:

i) Enhance the security of remote access to the corporate network.

ii) Restrict remote connections of Paramount Finance UK Ltd.'s to employees only.

(10 marks)

b) Using Paramount Finance UK Ltd.'s Network Architecture (Figure 1), design a new well-labelled network diagram:

i) To include Demilitarized Zone(s) (DMZs) to protect critical servers.

ii) Include VPNs for secure remote access for employees working off-site. Critical systems should also be identified.

(5 marks)

c) Explain in detail reasons for your chosen network design **and** the purpose/functions of the Demilitarized Zones (DMZs) **and** VPNs.

(10 marks)

Question 2 – 25 Marks

Paramount Finance UK Ltd has requested for a vulnerability assessment to be conducted on the web server.

a) Explain the difference between vulnerability management **and** vulnerability scanning.

(5 marks)

b) Explain the difference between known **and** unknown vulnerabilities **including** methods you will use to detect them on the web server.

(10 marks)

© NCC Education Limited 2021

c) Explain authentication **including** methods that can be used to improve password security **and** authentication on the company's web server.

(10 marks)

Question 3 – 25 Marks

Recently, the data of a competitor company was breached by hackers using a sophisticated phishing attack via email and data theft from storage devices. Paramount Finance UK Ltd is concerned about a similar breach.

a) Explain what a phishing attack is and discuss recommendations that should be implemented by Paramount Finance to prevent phishing attacks.

(10 marks)

b) Provide detailed recommendations that will protect devices such as laptops and removable media used by the company's employees for work against unauthorised access, data theft and deletion.

(10 marks)

c) Describe what a digital signature is and explain its role in the security of email communications.

(5 marks)

Question 4 – 25 Marks

There have been instances where files downloaded from the file servers have been modified or corrupt. One of the proposals by the Chief Information Officer (CIO) is to implement cryptography to ensure confidentiality, integrity, and authenticity of files hosted on the servers.

a) Explain the functions of hashing algorithms for file integrity **and** select an appropriate one best suited for employees to verify the integrity of downloaded files. You should provide justification for your selected algorithm.

(10 marks)

b) Explain Public Key Infrastructure (PKI) **and** its benefits to support secure information exchange over insecure networks.

(10 marks)

c) Suppose an employee off-site intends to access a file server remotely using a public Wi-Fi connection from a local café. Explain the vulnerabilities inherent in open-public wireless networks.

(5 marks)

End of paper

© NCC Education Limited 2021