KABARAK UNIVERSITY

UNIVERSITY EXAMINATIONS

2009/2010 ACADEMIC YEAR

FOR THE DEGREE OF BACHELOR OF BUSINESS MANAGEMENT & INFORMATION TECHNOLOGY

COURSE CODE: **BMIT 416**

COURSE TITLE: **IT SECURITY, AUDIT AND ETHICS**

STREAM: **Y4S1**

DAY: **MONDAY**

TIME: **2.00 – 5.00 P.M.**

DATE: **22/03/2010**

INSTRUCTIONS:

- SECTION A : Answer Question **1** (COMPULSORY)
- SECTION B: Answer any **three** questions.

PLEASE TURN OVER

SECTION A (Compulsory) Answer ALL Questions in this section

QUESTION ONE (40 MARKS)

a)

i). What is ARP spoofing [2 marks]

ii). Outline any FOUR symptoms of ARP spoofing [2 marks]

b)

i). State Kerckhoff's principle. Explain briefly why a cryptosystem designed by someone who follows this principle is likely to be stronger than one designed by someone who does not. [5 marks]

ii). Explain the main drawback of the onetime pad cryptosystem? [4 marks]

c) Consider the following hypothetical Kerberos simple authenticated dialogue between a client C requesting accesses to a server V

$$C \longrightarrow AS:\ ID_c \,\|\, P_c \,\|\, ID_v$$

$$AS \longrightarrow C:\ \text{Ticket}$$

$$C \longrightarrow V:\ ID_c \,\|\, \text{Ticket}$$

$$\text{Ticket} = E_{kv}[\ ID_c \,\|\, AD_c \,\|\, ID_v\ ]$$

Where C = Client, AS is authentication server, V is server, ID_c is identifier of user on C, ID_v is identifier of V, P_c is password of user on C, AD_c is network address of C, K_v is secret encryption key shared by AS and V and $\|$ is concatenation

i). Explain the events in this dialogue that leads to V granting the service requested by C [6 marks]

ii). Outline the problem with this authentication technique stating any threats probable [3 marks]

d) Explain the following DoS attacks. [8 marks]

i). Buffer overflow

ii). SYN Attack

iii). Teardrop Attack

iv). Smurf

e) Company Y has its web application and database servers placed in a DMZ, protected by a network firewall. Each packet sent/received from Internet to/from DMZ is filtered by the firewall according the following ruleset:

Order	**Protocol**	**Source Host**	**Source Port**	**Destination Host**	**Destination Port**	**Permit/Deny**
1	SMTP	MAIL_1	25	Any	Any	Permit
2	Any	Any	Any	GENITALIA	Any	Deny
3	SMTP	Any	Any	Any	25	Permit
4	Any	Any	Any	Any	Any	Deny

Rules are processed from top to bottom. When a match occurs rest of the rules is discarded.

i). Explain the implications of each of these rule sets [6 marks]

ii). Explain the current security risk of the servers in this DMZ taking the rule set into account? [2 Marks]

iii). How could you eliminate these risk? [2 Marks]

SECTION B Answer Any THREE Questions in this section

QUESTION TWO (20 MARKS)

a) Assuming you can do 2^{20} encryptions per second and the key size is 40 bits, how long would a brute force attack take? Give a scenario where this would be practical and another where it wouldn't. What happens if you double the key size? [8 marks]

b) You have intercepted a message encrytped with an affine cipher. The ciphertext starts with BBDJ and you know the plaintext starts with oops. Find the key. [8 marks]

c) Consider a language with three letters, a, b, and c, with frequencies .6, .3, and .1. Suppose that a long message (1000 characters) in this language is encrypted with a Vign`ere cipher and we plan to break it using a index of coincidence attack. About how big is the largest index of coincidence we are likely to see? [5 marks]

QUESTION THREE (20 MARKS)

a) Explain three types of attacks that can be made on packet filtering routers and explain the appropriate counter measures for each [12 marks]

b) Use the extended Euclidean algorithm to compute the greatest common divisor d of 654 and 123 and to find integers m and n such that 654m + 123n = d. [8 marks]

QUESTION FOUR (20 MARKS)

Outline the activities that take place during the following stages of a Kerberos authentication process

i). User Client-based Logon [3 marks]

ii). Client Authentication [6 marks]

iii). Client Service Authorization [5 marks]

iv). Client Service Request [6 marks]

QUESTION FIVE (20 MARKS)

a) Modern web browsers provide a number of features that help to protect your privacy and make your computer and your personally identifiable information more secure.
Explain the role of Privacy and security features in a web browser [2 marks]

i. Outline THREE categories of privacy features included in Internet Explorer [3 marks]
ii. Outline THREE categories of security features included in Internet Explorer [3 marks]

b)

i. You are a system administrator of a secondary school; one of the internet policy Statements states *'students should not view Web sites that contain violent or sexual content'*. State the feature of internet explorer that you might use to enforce this policy and explain how you can access it and use it to achieve the desired results [6 marks]

ii. Outline SIX activities that can be performed using the feature stated above to control access to the internet [6 marks]