STIJ3133

FINAL EXAM
FIRST SEMESTER SESSION 2011/2012

COURSE CODE / NAME : STIJ3133/ SYSTEM & NETWORK SECURITY
DATE : 10 JANUARY 2012 (TUESDAY)
TIME : 9.00 -11.30 a.m. (2½ HOURS)
VENUE : DTSO

INSTRUCTION :
1. This book script contains THIRTEEN (13) questions in TEN (10) printed pages excluding the cover page.
2. Answer ALL the questions in the spaces provided.

MATRIC NO : ____________________________ (with word)

IDENTIFICATION CARD NO : ____________ (with number)

LECTURER : ____________________________

GROUP : # TABLE NO : ____________

DO NOT OPEN THIS EXAMINATION PAPER UNTIL INSTRUCTED

CONFIDENTIAL
1. a) What is the difference between passive and active security threats?

   b) List and briefly define categories of security services.

   c) List and briefly define categories of security mechanisms.

   (8 marks)

2. a) What are the **TWO** (2) basic functions used in encryption algorithms?

   b) What is the difference between a block cipher and a stream cipher?
c) What are the **TWO (2)** general approaches to attacking a cipher?

d) What is triple encryption?

(8 marks)

3. Consider a very simple symmetric block encryption algorithm in which 32-bits blocks of plaintext are encrypted using a 64-bit key. Encryption is defined as

\[ C = (P \oplus K_0) \oplus K_1 \]

where \( C \) = ciphertext, \( K \) = secret key, \( K_0 \) = leftmost 64 bits of \( K \), \( K_1 \) = rightmost 64 bits of \( K \), \( \oplus \) = bitwise exclusive OR, and \( \oplus \) is addition mod 264. Show the decryption equation. That is, show the equation for \( P \) as a function of \( C \), \( K_0 \) and \( K_1 \).

(10 marks)
4. In a public-key system using RSA, you intercept the ciphertext $C=10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext $M$?

5. a) What is a key distribution center? 

b) What is a public-key certificate?
c) what is the purpose of the X.509 standard?

6. The ultimate goal of implementing security on a network is achieved by following FIVE (5) steps, each aimed at clarifying the relationship between the attacks and the measures that protect against them. List and briefly describe the steps.

7. List and briefly explain THREE(3) fundamental goals for computer security
8. a) How does PGP use the concept of trust?

b) What are the FIVE(5) principal services provided by PGP?

c) Describe briefly how the IPsec works.

d) Give THREE(3) examples of applications of IPsec.
9. a) What is the role of compression in the operation of a computer virus?

b) In general terms, how does a computer worm propagate?

(5 marks)

10. The following is a kind of social engineering message often received through our email:

From: 3dksobinsky@zoom-internet.net
Sent: Sunday, Nov 26, 2011 8:10 AM
To: rmstronger@charter.net
Subject: Re: Approved

Please read the attached file

Recommend a way to protect novel email users from being abused.

(10 marks)
11. Consider the following malicious code:

```vbscript
Private Declare Function GetAsyncKeyState Lib "user32" (ByVal vKey As Long) As Integer
Private Sub Timer1_Timer()
    For i = 1 To 255
        result = 0
        result = GetAsyncKeyState(i)
        If result = -32767 Then
            Text1.Text = Text1.Text + Chr(i)
        End if
        Next i
    End Sub
```

What will happen if the code is executed?

12. a) What is the difference between a packet filtering firewall and a stateful inspection firewall?
b) What is a DMZ network? What types of systems would you find on such networks?

(4 marks)

13. You are given the following "informal firewall policy" details to be implemented using a firewall shown in Figure 1:
STU3133 Keselamatan Sistem dan Rangkaian/System and Network Security

Figure 1

I. Email may be sent using SMTP in both directions through the firewall, but it must be relayed via the DMZ mail gateway that provides header sanitization and content filtering. External email must be destined for the DMZ mail server.

II. Users inside may retrieve their email from the DMZ mail gateway, using either POP3 or POP3S, and authenticate themselves.

III. Users outside may retrieve their email from the DMZ mail gateway, but only if they use the secure POP3S protocol, and authenticate themselves.

IV. Web requests (both insecure and secure) are allowed from any internal user out through the firewall but must be relayed via the DMZ Web proxy, which provides content filtering (noting this is not possible for secure requests), and user must authenticate with the proxy for logging.

V. Web requests (both insecure and secure) are allowed from anywhere on the Internet to the DMZ Web server.

VI. DNS lookup request by internal users allowed via the DMZ DNS Server, which queries to the Internet.

VII. External DNS requests are provided by the DMZ DNS Server.

VIII. Management and update of information on the DMZ Servers is allowed using secure shell connections from relevant authorized internal users (may have different sets of users on each system as appropriate).

IX. SNMP management requests are permitted from the internal management hosts to the firewalls, with the firewalls also allowed to send management traps (i.e., notification of some events occurring) to the management hosts.

Design suitable packet filter rulesets (using the table format shown in Figure 2) to be implemented on the “external firewall” and the “internal firewall” to satisfy the aforementioned policy requirements.

<table>
<thead>
<tr>
<th>RULE SET A</th>
<th>Action</th>
<th>Ourhost</th>
<th>Port</th>
<th>Theirhost</th>
<th>Port</th>
<th>comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RULE SET X</th>
<th>Action</th>
<th>Ourhost</th>
<th>Port</th>
<th>Theirhost</th>
<th>Port</th>
<th>Flags</th>
<th>comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 2.

(10 marks)
END OF QUESTIONS

10