UNIVERSITI TUN HUSSEIN ONN MALAYSIA

PEPERIKSAAN AKHIR
SEMESTER II
SESI 2008/ 2009

NAMA MATA PELAJARAN	:	KESELAMATAN RANGKAIAN
KOD MATA PELAJARAN	:	BIT 3323
KURSUS	:	3 BIT
TARIKH PEPERIKSAAN	:	APRIL/MEI 2009
JANGKA MASA	:	3 JAM
ARAHAN	:	JAWAB **SEMUA** SOALAN.

KERTAS SOALAN INI MENGANDUNGI LIMA (5) MUKA SURAT

Instruction: Answer **ALL** questions.

Q1 (a) Describe **TWO (2)** type of computer / information security attacks defined by X.800 and RFC 2828

(6 marks)

(b) Explain **THREE (3)** focuses in OSI security architecture based on *X.800 Recommendation*.

(6 marks)

(c) Define the following terms:

(i) Replay Attack
(ii) Data Origin Authentication
(iii) Traffic Analysis
(iv) Denial of Service

(8 marks)

Q2 (a) Explain how the RSA public and private keys are generated. Give any necessary equations with examples.

(6 marks)

(b) Describe the equation to encrypt a message M and to decrypt ciphertext of M to achieve confidentiality using RSA cryptosystem.

(6 marks)

(c) Give a method to achieve non-repudiation of transmission using RSA cryptosystem. Name **TWO (2)** factors on which the security of this methods depends.

(8 marks)

Q3 (a) Explain what spyware is and give **TWO (2)** examples.

(4 marks)

(b) Explain **FOUR (4)** steps that can be used to help reduce the threat of spyware and adware.

(8 marks)

(c) Aleeya is a network administrator for an insurance company. The company has 6 servers and 40 workstations. The claims department, in particular keeps sensitive documents on its workstations. Also most employees frequently use the Internet for work-related purposes. She takes the following actions to harden the operating systems of all servers and workstations:
Action 1 : She applies all patches and schedules to check patches every two month.
Action 2 : She disables default account on all machines.
Action 3 : She sets Internet Explorer to high security.

Explain **FOUR (4)** steps can be taken by Aleeya to harden the servers and workstations. (8 marks)

Q4 In order to protect a web server with an IP 10.5.4.254, system administrator installed firewall on the system with following rules as in **Figure Q4 (a)**. The rules allowing system administrator to use telnet for maintenance from his own PC with the IP 10.5.4.6.

```
Rules
Policy Drop
iptables -A INPUT –src 10.5.4.6 -dest 10.5.4.254 -p 23 -j ALLOW
iptables -A INPUT –src any -dest 10.5.4.254 -p 80 -j ALLOW
```

Figure Q4 (a)

(a) Explain **TWO (2)** advantages of this firewall.

(6 marks)

(b) Discuss how system administrator should improve this system to remotely access web server for maintenance.

(6 marks)

(c) Clarify **TWO (2)** differences between honeypot and firewall.

(8 marks)

Q5 (a) Explain what is IPsec.

(4 marks)

(b) IPsec provides choices of security service. Explain **TWO (2)** of them.

(4 marks)

(c) Explain how brute force attack works in cracking the password.

(4 marks)

(d) Mobile handsets are steadily increasing in functionality and flexibility, to the point where the handset is becoming a general purpose computing platform. Explain **FOUR (4)** new security issues that you think will arise in the future, as the complexity of mobile handsets increases.

(8 marks)

Arahan: Jawab **SEMUA** soalan.

S1 (a) Terangkan mengenai model keselamatan CIA di dalam bidang keselamatan Maklumat / Komputer.

(6 markah)

(b) Jelaskan **TIGA (3)** fokus persekitaran keselamatan OSI berdasarkan Cadangan X.800.

(6 markah)

(c) Definisikan terma-terma berikut:

(i) *Replay Attack*
(ii) *Data Origin Authentication*
(iii) *Traffic Analysis*
(iv) *Denial of Service*

(8 markah)

S2 (a) Jelaskan bagaimana pasangan kunci awam dan kunci persendirian dijana dalam enskripsi *RSA*. Beri persamaan-persamaan beserta contoh.

(6 markah)

(b) Nyatakan persamaan-persamaan untuk menyulitkan dan menyahsulitkan mesej M untuk mencapai kerahsiaanya menggunakan Sistem Kripto RSA.

(6 markah)

(c) (i) Nyatakan kaedah untuk mencapai tiada sangkalan dalam penghataran mesej menggunakan Sistem Kripto *RSA*

(4 markah)

(ii) Senaraikan **DUA (2)** faktor utama yang menjamin keselamatan Sistem Kripto *RSA*.

(4 markah)

S3 (a) Jelaskan apakah spyware dan berikan **DUA (2)** contoh.

(4 marks)

(b) Nyatakan **EMPAT (4)** langkah untuk mengurangkan spyware dan adware

(8 markah)

(c) Aleeya merupakan pentadbir rangkaian bagi sebuah syarikat insuran. Syarikat mempunyai 6 buah pelayan dan 40 buah stesen kerja. Bahagian Tuntutan biasanya menyimpan maklumat-maklumat yang sensitif didalam beberapa dokumen yang berada di dalam stesen kerja. Hampir kesemua pekerja syarikat insuran menggunakan Internet untuk kerja-kerja mereka. Jelaskan **EMPAT (4)** langkah yang boleh diambil oleh Aleyaa untuk meningkatkan lagi pelayan dan stesen-stesen kerja di syarikatnya.

(8 markah)

S4 Untuk melindungi pelayan web dengan IP 10.5.4.254, pentadbir sistem telah memasang dindingapi terhadap sistem dengan aturan seperti **Rajah S4** (a). Aturan tersebut membenarkan penggunaan aplikasi *telnet* oleh pentadbir sistem melalui komputernya dengan IP 10.5.4.6

```
Rules
Policy Drop
iptables -A INPUT –src 10.5.4.6 -desl 10.5.4.254 -p 23 -j ALLOW
iptables -A INPUT –src any -dest 10.5.4.254 -p 80 -j ALLOW
```

Rajah S4 (a)

(a) Jelaskan **DUA (2)** kelebihan *firewall* ini.

(6 markah)

(b) Bincangkan bagaimana pentadbir sistem boleh meningkatkan keselamatan sistem ini disamping membolehkan *remote access* kepada pelayan web untuk penyelenggaraan.

(6 markah)

(c) Nyatakan **DUA (2)** perbezaan diantara *honeypot* and *firewall*.

(8 markah)

S5 (a) Jelaskan apakah *IPsec*.

(4 markah)

(b) *IPsec* menyediakan pelbagai pilihan keselamatan. Jelaskan DUA (2) daripadanya.

(4 markah)

(c) Jelaskan bagaimana serangan *brute force* digunakan untuk mendedahkan katalaluan.

(4 markah)

(d) Fungsi dan fleksibiliti telefon mudah alih semakin meningkat akhir-akhir ini sehingga pengguna kini boleh kerja seperti sebuah komputer. Bincangkan **EMPAT (4)** isu-isu keselamatan maklumat yang anda jangka dihadapi oleh pengguna akibat peningkatan kemajuan telefon mudah alih.

(8 markah)