UNIVERSITI TUN HUSSEIN ONN MALAYSIA

PEPERIKSAAN AKHIR
SEMESTER I
SESI 2009/2010

NAMA MATA PELAJARAN : KESELAMATAN RANGKAIAN

KOD MATA PELAJARAN : BIT 3323

KURSUS : 3 BIT

TARIKH PEPERIKSAAN : NOVEMBER 2009

JANGKA MASA : 3 JAM

ARAHAN : JAWAB **SEMUA** SOALAN.

KERTAS SOALAN INI MENGANDUNGI TUJUH (7) MUKA SURAT

Instruction: Answer **ALL** questions.

Q1 Classify each of the following either as a violation of confidentiality, integrity or availability.

a) Shima tries to use her sister's matric card to go inside the lecturer room.

b) Tan breaks into the database server and try to modify his final exam result.

c) ABC company web site could not display certain information requested by the user.

d) Deli log in to company server and changed other staff confidential information.

e) Myra uses a tool available in the Internet to retrieve other user's password.

(5 marks)

Q2 (a) Describe **TWO (2)** techniques employed by hackers to gain access to passwords.

(4 marks)

(b) Elaborate how session cloning is done.

(4 marks)

(c) Recommend **THREE (3)** steps to defense against SQL injection

(6 marks)

(d) Propose **THREE (3)** steps to protect wireless communication against eavesdropping.

(6 marks)

Q3 (a) How can phishing mails be used to exploit internet banking?

(4 marks)

(b) Clarify **THREE (3)** ways that can be used to defense your network from war dialing.

(6 marks)

(c) Discuss **TWO (2)** ways that attacker can perform to harden the system which has been attacked by him.

(4 marks)

Q4 (a) Give **TWO (2)** steps on how to create your own remote control Application-Level Trojan Horse Backdoor Tools.

(2 marks)

(b) Give **TWO (2)** differences between worm and virus.

(4 marks)

(c) Clarify **TWO (2)** ways to avoid a virus from being spread.

(4 marks)

Q5 John is an attacker who manages to break into two servers that belong to Fartech Sdn. Bhd. He needs to hide all traces of his activities from the servers. Server A is using Red Hat Enterprise, while server B is using Windows 2003 Advanced Server Network Operating System (NOS).

(a) Elaborate how to hide intrusion traces and explain on what log files needed to be altered in:

(i) Server A (Red Hat Enterprise NOS)
(ii) Server B (Windows 2003 Advanced Server NOS)

(14 marks)

(b) Give **THREE (3)** suggestions to prevent attackers from hiding or wiping out their traces.

(6 marks)

Q6 There is an attempt to hack into DEF network. The hackers do not have any information on the existing network. Explain **FIVE (5)** steps how the hackers could penetrate the network.

(10 marks)

Q7 Acme corporation's network consists of router, firewall, web server, DNS server, file server in DMZ area and 10 hosts. The company also provides hotspot at the company's building. They are planning a public web server to provide publicly available information and a secure sub-site using SSL for transactions. The web server software and operating system are not considered secure. So the suggestion is to protect the web server with a network level firewall set to pass in port 80 traffic and to block all the incoming traffic. Outgoing traffic will not be restricted. The server will be completely isolated from the rest of Acme's network.

(a) Sketch the Acme corporation's network.

(6 marks)

(b) Comment on the security of this setup.

(5 marks)

(c) Create **FIVE (5)** action plans that should been taken to improve the security for the existing network using logical (not physical) methods.

(10 marks)

Arahan: Jawab **SEMUA** soalan.

S1 Nyatakan penyataan berikut samada dalam kategori kerahsiaan, integriti atau kebolehcapaian.

a) Shima cuba menggunakan kad matrik kakaknya untuk masuk ke dalam bilik pensyarah.

b) Tan memecah masuk ke dalam pelayan pangkalan data dan cuba mengubah markah peperiksaan akhirnya.

c) Laman sesawang Syarikat ABC tidak dapat memaparkan beberapa maklumat yang diminta oleh pengguna.

d) Deli mendaftar masuk ke dalam pelayan syarikat dan mengubah maklumat sulit pekerja lain.

e) Myra menggunakan peralatan yang dimuat turun daripada Internet untuk mendapatkan katalaluan pengguna lain.

(5 markah)

S2 (a) Huraikan **DUA (2)** kaedah yang digunakan oleh penggodam untuk mendapatkan katalaluan.

(4 markah)

(b) Bincangkan bagaimana *session cloning* dilakukan.

(4 markah)

(c) Cadangkan **TIGA (3)** langkah untuk mempertahankan rangkaian daripada *SQL injection.*

(6 markah)

(d) Cadangkan **TIGA (3)** langkah untuk melindungi komunikasi tanpa wayar dari diintip.

(6 markah)

S3 (a) Terangkan bagaimana emel *phishing* boleh digunakan untuk merosakkan perbankan Internet.

(4 markah)

(b) Huraikan **TIGA (3)** cara untuk mempertahankan rangkaian daripada *war dialing.*

(6 markah)

(c) Bincangkan **DUA (2)** cara yang dilakukan oleh penggodam untuk memperkuatkan sistem yang telah ditembusi olehnya.

(4 markah)

S4 (a) Terangkan **DUA (2)** langkah membuat peralatan kawalan remot *Application-Level Trojan Horse Backdoor* tanpa pengetahuan pengaturcaraan.

(2 markah)

(b) Berikan **DUA (2)** perbezaan antara cecacing dan virus.

(4 markah)

(c) Terangkan DUA (2) kaedah untuk mengelakkan virus daripada tersebar.

(4 markah)

S5 John berjaya memecah masuk ke dua buah komputer pelayan milik Fartech Sdn Bhd. Beliau perlu menyembunyikan jejak aktivitinya daripada komputer pelayan. Komputer pelayan A menggunakan Sistem Pengoperasian Rangkaian *Red Hat Enterprise*, manakala komputer pelayan B menggunakan *Windows 2003 Advanced Server Network.*

(a) Huraikan bagaimana menyembunyikan jejak penggodam ke atas fail log di:

(i) Komputer Pelayan A (Sistem Pengoperasian Rangkaian *Red Hat Enterprise*).
(ii) Komputer Pelayan B (Sistem Pengoperasian Rangkaian *Windows 2003 Advanced Server*).

(14 markah)

(b) Berikan **TIGA (3)** cadangan untuk mengelakkan penggodam menyembunyikan atau menghilangkan jejak mereka.

(6 markah)

S6 Terdapat percubaan untuk memecah masuk ke dalam rangkaian DEF. Walaubagai manapun, penggodam tersebut tidak mempunyai sebarang maklumat berkaitan dengan rangkaian semasa. Terangkan **LIMA (5)** langkah bagaimana penggodam boleh menembusi rangkaian DEF.

(10 markah)

S7 Rangkaian *Acme Corporation* mengandungi *router, firewall*, pelayan web, pelayan DNS, pelayan fail di kawasan DMZ dan 10 buah komputer. Syarikat ini juga menyediakan kemudahan *hotspot*. Mereka merancang untuk mempunyai sebuah pelayan web awam yang akan menyediakan maklumat dan laman transaksi selamat menggunakan SSL. Perisian pelayan web dan sistem pengoperasian tidak dianggap selamat. Untuk melindungi pelayan web, firewall ditetapkan untuk melepaskan port 80 dan menghalang semua trafik yang masuk ke dalam rangkaian. Walau bagaimanapun, trafik keluar tidak akan dihalang. Pelayan itu akan diletakkan berasingan dengan rangkaian Acme.

(a) Lakarkan rangkaian *Acme Corporation*.

(6 markah)

(b) Berikan komen terhadap keselamatan rangkaian yang dibangunkan.

(5 markah)

(c) Cadangkan **LIMA (5)** langkah yang patut diambil untuk meningkat keselamatan rangkaian sedia ada menggunakan kaedah logikal.

(10 markah)