UNIVERSITI SAINS MALAYSIA

Second Semester Examination
[Peperiksaan Semester Kedua]

Academic Session 2007/2008
[Sidang Akademik 2007/2008]

April 2008

CST334 – Network Monitoring and Security
[Pengawasan dan Keselamatan Rangkaian]

CST314 – Network Management and Security
[Pengurusan dan Keselamatan Rangkaian]

Duration : 2 hours
[Masa : 2 jam]

INSTRUCTIONS TO CANDIDATE:
[ARAHAN KEPADA CALON:]

- Please ensure that this examination paper contains **SIX** questions in **FIVE** printed pages before you begin the examination.

  *[Sila pastikan bahawa kertas peperiksaan ini mengandungi **ENAM** soalan di dalam **LIMA** muka surat yang bercetak sebelum anda memulakan peperiksaan ini.]*

- Answer **ALL** questions.

  *[Jawab **SEMUA** soalan.]*

- You may answer the questions either in English or in Bahasa Malaysia.

  [Anda dibenarkan menjawab soalan sama ada dalam Bahasa Inggeris atau Bahasa Malaysia.]

---

1. Please list and describe **three (3)** main differences between Worms and Viruses.

(10/100)

2. You are provided with a real-time Network Analyser. You are a system administrator. Your network currently is facing problems of high usage and congestion. You suspect that someone is using your Internet Access to download movies using peer-to-peer Software. Describe how you will use the Network Analyser to solve this problem via the following steps. Use diagrams to explain your results.

   (a) Where is the optimal place to put the analyser so that it can monitor the traffic going out and coming in from the Internet?

   (b) What Layer 3 protocol will you set the filter to look for?

   (c) How will you detect who the end user is?

(20/100)

3. Provide the names of any **three (3)** worms and the following description for each of the worms:

   (a) Name of worm.

   (b) A brief description.

   (c) Possible names.

   (d) Damaging effect.

(20/100)

4. The School of Computer Sciences wishes to upgrade and protect their network from intrusions by external users. This new upgrade will only enable Internet web server (port 80) access for the School's users. But the School of Computer Sciences has only one public IP address.

    (a) What is the network edge device that should be used to overcome the above situation, that is, using one IP to service the entire staff of the School of Computer Sciences?

    (b) Provide a brief explanation on how this device is used to carry out this function. Use diagrams to assist with the description.

    (c) What is the name of the network edge device that will work with the device from question 4(a) but its main function is to provide security by checking and filtering packets that come into the network?

(20/100)

5. (a) Explain how a hacker can steal the <username> and <password> of the user of a bank's website if this hacker can penetrate and enter the Internet edge router in USM. Use diagrams to help explain your answer.

    (b) What is the command used in:

    (i) Windows, and

    (ii) LINUX

    to show the user the IP address of the computer and the IP address of the gateway router it is connected to?

    (c) What is the name of the ministry that is responsible for the telecommunications sector in Malaysia in 2007? What is the name of the commission that handles ISP related regulations in Malaysia?

(15/100)

6. (a) Name **four (4)** network devices that are used for network security. Briefly describe each device's function.

    (b) State the ports used for `http`, `https`, `ssh` and `telnet` protocols.

(15/100)

KERTAS SOALAN DALAM VERSI BAHASA MALAYSIA

1. Senaraikan **tiga (3)** perbezaan utama di antara Ulat Komputer dan Virus Komputer.

(10/100)

2. Anda diberi sebuah Penganalisis Rangkaian Masa Nyata. Anda bekerja sebagai Pentadbir Sistem dan rangkaian anda ditimpa masalah kegunaan tinggi dan kesesakan. Anda mensyaki bahwa pengguna Internet anda sedang menggunakan akses Internet untuk muat turun wayang dengan menggunakan perisian berasas 'peer-to-peer'. Huraikan bagaimana anda akan menggunakan Penganalisis Rangkaian tersebut untuk mengatasi masalah ini dengan menggunakan langkah-langkah berikut. Guna gambar rajah untuk menjawab.

   (a) Di manakah tempat optimal untuk meletak alat penganalisis tersebut supaya ia dapat memantau trafik yang keluar serta masuk ke dalam rangkaian anda daripada Internet?

   (b) Protokol Lapisan 3 yang manakah akan anda memantau?

   (c) Bagaimanakah anda akan mengesan siapakah pengguna perisian 'peer-to-peer' tersebut?

(20/100)

3. Berikan nama mana-mana **tiga (3)** ulat komputer serta huraikannya mengikut berikut:

   (a) Nama ulat komputer.

   (b) Penerangan ringkas tentang ulat komputer tersebut.

   (c) Lain-lain nama ulat komputer tersebut.

   (d) Kesan-kesan kerosakan oleh ulat komputer tersebut.

(20/100)

4. Pusat Pengajian Komputer ingin menaiktaraf dan melindungi rangkaian mereka daripada pencerobohan oleh pengguna luaran. Rangkaian yang baru ini hanya akan membolehkan pelayan Web Internet (port 80) mencapai pengguna di dalam Pusat Pengajian. Walau bagaimanapun Pusat Pengajian Sains Komputer hanya mempunyai satu IP publik sahaja.

    (a) Apakah nama peralatan pinggiran rangkaian yang digunakan untuk mengatasi situasi di atas? Iaitu menggunakan satu IP untuk perkhidmatan seluruh staf Pusat Pengajian Sains Komputer.

    (b) Beri keterangan ringkas bagaimana peralatan ini digunakan untuk menjalankan fungsi tersebut.

    (c) Apakah nama peralatan pinggiran rangkaian yang akan bekerja dengan peralatan pada soalan 4(a) tetapi fungsi utamanya ialah memberi keselamatan dengan memeriksa dan menapis paket yang datang ke dalam rangkaian?

(20/100)

5. (a) Terangkan bagaimana penggodam boleh mencuri <nama pengguna> dan <kata laluan> satu pengguna laman web Bank apabila penggodam ini dapat menembusi dan masuk ke dalam penghala pinggiran Internet USM. Guna gambar rajah untuk membantu jawapan anda.

    (b) Apa perintah yang digunakan dalam:

        (i) Windows, dan

        (ii) LINUX

    untuk menunjukkan pengguna alamat IP komputer dan alamat IP penghala laluan get ianya tersambung?

    (c) Apakah nama kementerian bertanggungjawab untuk sektor telekomunikasi di Malaysia bagi tahun 2007? Apakah nama komisyen menangani regulasi berkaitan ISP di Malaysia?

(15/100)

6. (a) Namakan **empat (4)** peralatan rangkaian yang digunakan untuk keselamatan rangkaian. Terangkan dengan ringkas fungsi setiap peralatan tersebut.

    (b) Nyatakan port yang digunakan untuk protokol `http`, `https`, `ssh` dan `telnet`.

(15/100)

- oooOooo -