UNIVERSITI SAINS MALAYSIA

First Semester Examination
2014/2015 Academic Session

December 2014/January 2015

CST334 – Network Monitoring & Security
[Pengawasan & Keselamatan Rangkaian]

Duration : 2 hours
[Masa : 2 jam]

INSTRUCTIONS TO CANDIDATE:
[ARAHAN KEPADA CALON:]

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

  *[Sila pastikan bahawa kertas peperiksaan ini mengandungi **EMPAT** soalan di dalam **TUJUH** 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.]

- In the event of any discrepancies, the English version shall be used.

  [Sekiranya terdapat sebarang percanggahan pada soalan peperiksaan, versi bahasa Inggeris hendaklah diguna pakai.]

1. (a) Describe the three-way handshake process used to initiate TCP connections.

(3/100)

(b) What are some of the benefits of a layered architecture model?

(3/100)

(c) Your boss wants to know how subnetting works.

(i) Provide her with a brief description on how subnetting works.

(4/100)

(ii) Prepare an example to illustrate how subnetting works.

(6/100)

(d) (i) Why is it problematic to send confidential information over e-mail?

(2/100)

(ii) What is a solution to this problem?

(2/100)

(iii) What elements are almost always present in an effective hoax e-mail? Give an example.

(5/100)

2. (a) Your Web site is completely encrypted using SSL.

(i) How does this enhance security?

(4/100)

(ii) What will it not protect against?

(2/100)

(b) (i) What are cookies used for on a Web site, and what problem do they specifically address?

(4/100)

(ii) If your firm decides to go “cookieless,” what are the implications for your e-Commerce site?

(2/100)

(c) Identify the type of information that attackers might try to obtain if they were able to install a sniffer on a network.

(4/100)

(d) Explain the steps in spoofing a system across the Internet.

(9/100)

3. (a) You have just been asked to deploy an IDS at your company. The company has 500 desktops, 20 servers, and two connections to the Internet.

(i) Describe which type of IDS you would deploy and why.

(4/100)

(ii) Create network diagrams to show placement of components.

(4/100)

(iii) Describe how the system would be installed, maintained, and monitored.

(4/100)

(b) (i) Explain what is stateful inspection?

(5/100)

(ii) How is **state information** maintained during a network connection or transaction?

(2/100)

(c) Explain how the various types of firewalls interact with the network traffic at various levels of the OSI model.

(6/100)

4. (a) (i) What is the difference between a denial-of-service attack and a distributed denial-of-service attack?

(2/100)

(ii) Which is potentially more dangerous and devastating? Why?

(3/100)

(b) What is a buffer overflow and how is it used against a web server?

(3/100)

(c) Your company's security team wants more information about possible wireless solutions. They feel that WEP is secure because encryption can be used at 128 bits. Explain to them what the primary weakness in the WEP protocol is and how can it be exploited.

(4/100)

(d) Your company's management is considering rolling out 802.11 wireless and would like your input on what to choose. Describe the different.802.11 protocols and what has made them so popular, concluding with your recommendation to the management team.

(9/100)

(e) Imagine you are a Web developer for a small locally owned business.

(i) Explain when using HTTP would be satisfactory.

(2/100)

(ii) Explain when you should use HTTPS.

(2/100)

1. (a) Terangkan proses jabat tangan tiga hala yang digunakan dalam memulakan sambungan-sambungan TCP.

(3/100)

(b) Apakah manfaat-manfaat sebuah model seni bina berlapis?

(3/100)

(c) Majikan anda mahu tahu bagaimana pesubrangkaian dibuat.

(i) Berikan keterangan ringkas kepadanya bagaimana pesubrangkaian dibuat.

(4/100)

(ii) Sediakan satu contoh untuk menggambarkan bagaimana pesubrangkaian dibuat.

(6/100)

(d) (i) Mengapa ianya suatu masalah untuk menghantar maklumat sulit menerusi emel?

(2/100)

(ii) Apakah satu penyelesaian untuk masalah ini?

(2/100)

(iii) Apakah unsur-unsur yang sentiasa ada dalam satu emel palsu yang berkesan? Berikan satu contoh.

(5/100)

2. (a) Laman sesawang anda dienkripkan secara lengkap menggunakan SSL.

(i) Bagaimana ianya mempertingkatkan lagi keselamatan?

(4/100)

(ii) Apakah perkara yang ianya tidak akan lindungi?

(2/100)

(b) (i) Apakah (maksud) *cookie* yang digunakan untuk sesebuah laman sesawang, dan apakah masalah spesifik yang dikendalikan olehnya?

(4/100)

(ii) Jika firma anda memutuskan untuk tidak menggunakan “cookie”, apakah kesannya ke atas laman e-Dagang?

(2/100)

(c) Kenalpasti jenis maklumat yang akan cuba diperolehi oleh penyerang jika mereka dapat memasang *sniffer* dalam sesebuah rangkaian.

(4/100)

(d) Terangkan langkah-langkah dalam perdayaan sesebuah system menerusi Internet.

(9/100)

3. (a) Anda telah diminta memasang atur suatu ID di syarikat anda. Syarikat itu mempunyai 500 komputer meja, 20 pelayan, dan dua sambungan ke Internet.

(i) Terangkan jenis IDS yang akan anda pasang atur dan mengapa.

(4/100)

(ii) Cipta gambar rajah rangkaian untuk menunjukkan penempatan komponen-komponen berkaitan.

(4/100)

(iii) Terangkan bagaimana sistem tersebut akan dipasang, diselenggarakan, dan dipantau.

(4/100)

(b) (i) Terangkan apakah penyemakan berkeadaan?

(5/100)

(ii) Bagaimana maklumat keadaan diselenggarakan semasa satu sambungan rangkaian atau transaksi?

(2/100)

(c) Terangkan bagaimana pelbagai jenis tembok api berinteraksi dengan trafik rangkaian pada pelbagai tahap model OSI.

(6/100)

4. (a) (i) Apakah perbezaan antara suatu serangan nafi khidmat dan suatu serangan nafi khidmat teragih?

(2/100)

(ii) Yang mana satu berpotensi lebih merbahaya dan mengakibatkan kemusnahan? Mengapa?

(3/100)

(b) Apakah suatu limpahan penimbal dan bagaimana ianya digunakan ke atas sesebuah pelayan sesawang?

(3/100)

(c) Pasukan keselamatan syarikat anda mahukan lebih maklumat berkenaan dengan penyelesaian-penyelesaian tanpa wayar yang mungkin. Mereka merasakan bahawa WEP lebih selamat kerana enkripsi boleh digunakan pada 128 bit. Terangkan kepada mereka apakah kelemahan utama dalam protokol WEP dan bagaimana ianya boleh dieksploitasikan.

(4/100)

(d) Pengurusan syarikat anda mempertimbangkan untuk memperkenalkan tanpa wayar 802.11 dan mahukan input anda untuk mereka membuat pilihan. Jelaskan perbezaan protokol-protokol 802.11 dan apa yang membuatkannya begitu popular, dan akhiri dengan syor anda kepada pasukan pengurusan.

(9/100)

(e) Bayangkan anda adalah seorang pembangun sesawang untuk sebuah perniagaan kecil tempatan.

(i) Jelaskan bila penggunaan HTTP akan memadai.

(2/100)

(ii) Jelaskan bila sepatutnya ada gunakan HTTPS.

(2/100)