UNIVERSITI SAINS MALAYSIA

First Semester Examination
2016/2017 Academic Session

December 2016 / January 2017

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 **NINE** printed pages before you begin the examination.

  *[Sila pastikan bahawa kertas peperiksaan ini mengandungi **EMPAT** soalan di dalam **SEMBILAN** 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) (i) The Open Systems Interconnection model (OSI model) is a product of the Open Systems Interconnection effort at the International Organization for Standardisation (ISO). It is a way of sub-dividing a communications system into smaller parts called layers. Explain the concept of ***layer*** and ***layered architecture*** in this context.

*Model Sistem-Sistem Terbuka Berhubungan (model OSI) adalah satu produk kepada usaha Sistem-Sistem Terbuka Berhubungan di Organisasi Antarabangsa for Piawaian (ISO). Ianya adalah satu cara membahagi-bahagikan satu sistem komunikasi kepada bahagian-bahagian yang lebih kecil yang dipanggil lapisan-lapisan. Terangkan konsep **lapisan** dan **seni bina berlapisan** dalam konteks ini.*

(4/100)

(ii) In general, encapsulation is the inclusion of one thing within another thing so that the included thing is not apparent. Decapsulation is the removal or the making apparent a thing previously encapsulated. Briefly describe ***encapsulation*** in ***networking***. Give a proper example in your explanation.

*Pada umumnya, enkapsulasi adalah pemasukan satu perkara ke dalam perkara yang lain agar perkara yang dimasukkan itu tidak ketara. Dekapsulasi adalah pembuangan atau menjadikan ketara sesuatu perkara yang sebelumnya dienkapsulasikan. Terangkan dengan ringkas **enkapsulasi** dalam **perangkaian**. Berikan satu contoh yang sesuai dalam penjelasan anda.*

(4/100)

(b) Your boss wants to know how subnetting works. Provide her with a brief description and be sure to include an example to illustrate how subnetting works.

Majikan anda ingin tahu bagaimana pesubrangkaianan berfungsi. Berikan beliau satu keterangan ringkas dan pastikan anda memasukkan satu contoh untuk menggambarkan bagaimana pesubrangkaianan berfungsi.

(10/100)

(c) (i) What is an open port?

Apakah suatu pangkalan terbuka?

(2/100)

(ii) Why is it important to limit the number of open ports a system has to only those that are absolutely essential?

Mengapa ianya adalah mustahak mengehadkan bilangan pangkalan-pangkalan terbuka sesebuah sistem kepada hanya yang benar-benar perlu sahaja?

(2/100)

(d) Trusted Computer Base (TCB) is considered the totality of protection mechanisms within a computer system and is responsible for enforcing security. Why?

Asas Komputer Dipercayai (TCB) dipertimbangkan sebagai mekanisme perlindungan menyeluruh dalam sesebuah sistem komputer dan bertanggungjawab dalam menguatkuasakan keselamatan. Mengapa?

(3/100)

2. (a) You are a network administrator at a company. There is a database server that stores accounting data, customer data, and employee data. There is also a web server that must be accessed by customers and employees. Some employees work remotely and need access to an FTP server to upload and download files. The company uses Microsoft Exchange for email.

Anda adalah pengurus rangkaian sebuah syarikat. Terdapat satu pelayan pangkalan data yang menyimpan data perakaunan, data pelanggan, dan data pekerja. Terdapat juga satu pelayan sesawang yang mesti dicapai oleh pelanggan dan pekerja. Beberapa pekerja bekerja secara jauh dan perlukan capaian ke atas sebuah pelayan FTP untuk memuat naik dan memuat turun fail-fail. Syarikat anda menggunakan Microsoft Exchange untuk emel.

(i) Describe the justification for running FTP and the web service on different servers.

Jelaskan justifikasi untuk mengendalikan servis FTP dan sesawang pada pelayan-pelayan yang berbeza.

(2/100)

(ii) The table below lists some well-known ports and some servers. Identify whether the ports should be open or closed.

Jadual di bawah menyenaraikan beberapa pangkalan yang terkenal dan beberapa pelayan. Kenal pasti pangkalan-pangkalan yang mesti dibuka dan ditutup.

Ports	Exchange server	Domain controller	Web server	FTP server	Database server
20	**Closed**				
21		**Closed**			
23			**Closed**		
25				**Closed**	
80					**Closed**

(10/100)

(iii) Describe the danger port scanners pose to your network.

Terangkan bahaya pengimbas-pengimbas pangkalan ke atas rangkaian anda.

(2/100)

(iv) You decide to segment your network using a DMZ. Which servers should you place in the DMZ?

Anda memutuskan untuk mensegmenkan rangkaian anda menggunakan satu DMZ. Pelayan-pelayan apakah yang sepatutnya diletakkan dalam DMZ berkenaan.

(2/100)

(v) What is one way you can allow the Microsoft Exchange server to receive email from an SMTP forwarder on the Internet?

Apakah satu kaedah yang membolehkan anda membenarkan pelayan Microsoft Exchange menerima emel daripada satu penghantar SMTP ke Internet?

(2/100)

(vi) Which servers should include a modem in the scenario?

Pelayan-pelayan manakah yang sepatutnya dimasukkan sebuah modem dalam senario ini?

(1/100)

(vii) The database servers are in a locked closet on the internal network. How should you apply access permissions to add another layer of depth to the database servers' defense?

Pelayan-pelayan pangkalan data berada dalam ruang perabot berkunci dalam rangkaian dalaman. Bagaimanakah sepatutnya anda melaksanakan kebenaran-kebenaran capaian untuk menambah satu lagi lapisan kedalaman pertahanan kepada pelayan-pelayan pangkalan data tersebut?

(1/100)

(b) (i) The popularity of searching for and attacking wireless networks has increased greatly in the last few years. Explain the possible reason for this phenomenon.

Populariti mengimbas dan menyerang rangkaian-rangkaian tanpa wayar telah bertambah dengan cepat dalam beberapa tahun kebelakangan. Terangkan sebab yang mungkin kepada fenomena ini.

(2/100)

(ii) Why is 802.11 wireless network more of a security problem than any other type of network?

Mengapa rangkaian tanpa wayar 802.11 lebih merupakan satu masalah keselamatan berbanding dengan rangkaian jenis lain?

(2/100)

(iii) Wireless Transport Layer Security (WTLS) must have support for short key lengths thus limiting the amount of security the protocol can provide. Identify the major cause for this.

WTLS mesti mempunyai sokongan untuk kepanjangan kunci pendek yang mana mengehadkan kadar keselamatan yang boleh diberikan oleh protokol berkenaan. Kenal pasti sebab utama perkara ini.

(1/100)

3. (a) SFRGcorp has asked you to recommend a strategy for detecting possible attacks on the network. SFRGcorp has hired a security team of 2 people. Part of their jobs will be to watch for signs that indicate an attack. SFRGcorp's development team builds web applications for customers and deploys them on a perimeter network. Each application will have a different network access pattern. One of SFRGcorp's concerns is that a detection system will trigger false alarms when a new customer application is deployed.

SFRGcorp meminta anda mencadangkan satu strategi untuk mengesan kemungkinan-kemungkinan serangan ke atas rangkaian. SFRGcorp telah melantik satu pasukan keselamatan dengan dua anggota. Sebahagian daripada kerja mereka adalah memantau tanda-tanda yang menunjukkan sesuatu serangan. Pasukan pembangun SFRGcorp membina aplikasi sesawang untuk pelanggan-pelanggan dan meletakkannya pada satu perimeter rangkaian. Setiap aplikasi akan mempunyai satu corak capaian rangkaian yang berbeza. Salah satu daripada perkara yang diambil berat oleh SFRG adalah satu sistem pengesan yang akan mencetus penggera-penggera palsu apabila suatu aplikasi pelanggan yang baru dipasang.

(i) Compare a **signature-based IDS** with an **anomaly-based IDS**.

*Bandingkan suatu **IDS berasaskan-tanda** dengan suatu **IDS berasaskan-penyimpangan**.*

(2/100)

(ii) Compare a **network-based IDS** and a **host-based IDS**.

*Bandingkan suatu **IDS berasaskan-rangkaian** dan suatu **IDS berasaskan-hos**.*

(2/100)

(iii) What type of intrusion detection will you recommend for the above situation? Explain why.

Apakah jenis pengesan pencerobohan yang akan anda cadangkan untuk situasi di atas? Terangkan mengapa.

(2/100)

(iv) What would be the maintenance concern for this type of IDS?

Apakah yang akan menjadi pertimbangan dalam penyelenggaraan IDS jenis ini?

(1/100)

(b) (i) Explain the difference between a **gateway** and a **firewall**.

*Terangkan perbezaan antara **get laluan** dan **tembok api**.*

(2/100)

(ii) How is a **circuit gateway** different from the other types of **firewalls**?

*Bagaimana satu **get laluan litar** berbeza dengan bentuk-bentuk lain **tembok api**?*

(4/100)

(c) **Disclosure attacks** seek to gain access to systems and information that should not be available to unauthorized individuals. Describe the following disclosure attacks and their potential effects.

***Serangan-serangan pendedahan** mencari cara untuk mendapat capaian kepada sistem-sistem dan maklumat yang tidak sepatutnya tersedia untuk individu-individu yang tidak dibenarkan. Terangkan serangan-serangan pendedahan berikut dan potensi kesan-kesannya.*

(i) Sniffing.

Penghiduan.

(3/100)

(ii) DNS spoofing.

Perdayaan DNS.

(3/100)

(iii) Pharming attack

Serangan Pharming.

(3/100)

(iv) Phishing attack

Serangan Pemancingan Data.

(3/100)

4. (a) ForensicCorp provides accounting, web development, and marketing services for over 200 small businesses. ForensicCorp 's network is configured as a single subnet with a bastion host firewall providing perimeter protection between the internal network and the Internet. The CEO is concerned about the company's liability if customer records were obtained. Customers currently upload their records to an FTP server hosted by ForensicCorp 's ISP. After the records have been uploaded, they are downloaded by one of 10 data entry people and entered into a database. The data is then retrieved and manipulated by one of 4 accountants. The accountants handle accounts receivable, accounts payable, reporting, and tax form generation for the companies. No other ForensicCorp employees should have access to the data.

ForensicCorp memberikan perkhidmatan-perkhidmatan perakaunan, dan pembangunan sesawang kepada lebih daripada 200 perniagaan kecil. Rangkaian ForensicCorp dikonfigurasikan sebagai satu sub rangkaian tunggal dengan satu hos benteng tembok api yang memberikan perimeter perlindungan antara rangkaian dalaman dan Internet. CEO mengambil berat tentang tanggungjawab syarikat sekiranya rekod-rekod pelanggan diperoleh oleh pihak lain. Pada keadaan semasa para pelanggan memuat naik rekod-rekod mereka menerusi satu pelayan FTP yang dihoskan oleh ISP ForensicCorp. Setelah rekod-rekod dimuat naik, mereka dimuat turun oleh satu daripada 10 pekerja kemasukan data dan dimasukkan ke dalam pangkalan data. Data berkenaan kemudiannya didapatkan kembali dan diolah oleh satu daripada 14 akauntan. Para akauntan mengendalikan akaun-akaun boleh diterima, akaun-akaun boleh dibayar, laporan, dan penjanaan borang cukai untuk syarikat-syarikat tersebut. Tiada seorangpun pekerja lain ForensicCorp yang sepatutnya dapat mencapai data-data berkenaan.

(i) Which threat or threats provide(s) the greatest risk to customer accounting data?

Ancaman atau ancaman-ancaman manakah yang menyebabkan risiko yang amat besar ke atas data perakaunan pelanggan?

(2/100)

(ii) What step could you take to secure the data while it is being transmitted by the customer?

Apakah langkah yang akan anda ambil untuk melindungi data semasa ianya dihantar oleh pelanggan?

(1/100)

(iii) How could you change your network segments to protect the data before it is downloaded by data entry personnel?

Bagaimana anda boleh mengubah segmen-segmen rangkaian berkenaan untuk melindungi data sebelum ianya dimuat turun oleh pekerja kemasukan data?

(2/100)

(iv) What steps involving the network can you take to protect the database server?

Apakah langkah-langkah yang melibatkan rangkaian yang boleh anda ambil untuk melindungi pelayan pangkalan data?

(3/100)

(v) What steps can you take to protect the data when it is being transmitted between the database server and the accountants' computers?

Apakah langkah-langkah yang boleh diambil untuk melindungi data apabila ianya dihantar antara pelayan pangkalan data dan computer akauntan?

(2/100)

(vi) What would prevent you from using SSL?

Apakah yang boleh menghalang anda daripada menggunakan SSL?

(2/100)

(b) (i) Explain how, by applying both asymmetric and symmetric encryption, your browser uses SSL to protect the privacy of the information passing between your browser and a Web server.

Terangkan bagaimana, dengan menggunakan enkripsi asimetrik dan simetrik, perambang anda menggunakan SSL untuk melindungi privasi maklumat yang dihantar antara perambang ada dan pelayan sesawang.

(3/100)

(ii) It is well understood that asymmetric encryption consumes more computing resources than symmetric encryption. Explain how PGP uses both asymmetric and symmetric encryption to be both secure and efficient.

Ianya jelas difahami bahawa enkripsi asimetrik menggunakan lebih sumber pengkomputeran berbanding enkripsi simetrik. Terangkan bagaimana PGP menggunakan kedua-dua enkripsi asimetrik dan simetrik untuk lebih selamat dan berkesan.

(5/100)

(c) Nik Anas has noticed a high level of TCP traffic in and out of the network. After running a packet sniffer, he discovered malformed TCP ACK packets with unauthorized data. We can classify what Nik Anas discovered as a covert channel.

Nik Anas memerhatikan terdapat satu tahap peningkatan trafik TCP ke dalam dan ke luar rangkaian. Selepas melaksanakan satu penghidu paket, beliau mendapati paket-paket TCP ACK cacat dengan data yang tidak dibenarkan. Kita boleh mengelaskan apa yang dijumpai oleh Nik Anas sebagai suatu saluran pendambaan.

(i) Why is the case considered a covert channel and not a buffer overflow?

Mengapa kes berkenaan dipertimbangkan sebagai suatu saluran pendambaan dan bukan suatu limpahan penimbal?

(2/100)

(ii) Why is it that we cannot classify the attack as a DoS attack?

Mengapa kita tidak boleh mengelaskan serangan berkenaan sebagai satu serangan DoS?

(1/100)

(iii) Explain how availability is a security concern.

Terangkan bagaimana aspek kesediaan adalah satu pertimbangan keselamatan.

(2/100)