UNIVERSITI SAINS MALAYSIA

First Semester Examination
2015/2016 Academic Session

December 2015/January 2016

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

  *[Sila pastikan bahawa kertas peperiksaan ini mengandungi **EMPAT** soalan di dalam **SEBELAS** 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) A developer in your company is building a new application and has asked you if the application should use TCP- or UDP-based communications. Explain to the developer on the advantages and disadvantages of each protocol.

(8/100)

(b) Your boss wants to know if DHCP can be appropriately used for both **server** and **PC environments**. Provide your opinion and be sure to explain on how DCHP works to defend your position.

(6/100)

(c) Your company, ABC Plastics, is a firm that buys plastic resin from manufacturers and sells it to small users. To be competitive, your firm needs to conduct business via the Internet, and along these lines has decided to connect its internal network, consisting of an e-mail server, a file server, and a database server to the Internet. To facilitate B2B transaction processing, a Web server and application server are being added to the network. The company understands the critical nature associated with this change and has initiated a project under your direction to design the new environment.

Describe the security topology you would recommend in this instance. Also, explain where each server should be located in the network, and the rationale behind the placement decision.

(7/100)

(d) Network Address Translation (NAT) is the protocol which can be used to translate private (non-routable) IP addresses into public (routable) IP addresses. Explain the **two** (**2**) purposes of the NAT service?

(4/100)

2. (a) You have been asked to write a security policy regarding wireless-based e-mail for your corporation. Explain in the policy why you would or would not allow confidential information to be sent over this medium.

(4/100)

(b) There are various technologies employed by wireless devices to maximize their use of the available radio frequencies. List and describe briefly **three** (**3**) of the technologies.

(6/100)

(c) You are installing a wireless network in your apartment and will be performing work-related functions on days when you telecommute from home. List and describe briefly with proper example **two** (**2**) basic steps you should take to protect your wireless network from potential unauthorized user access in your apartment complex.

(4/100)

(d) Consider the following security steps or policies:

- Install a firewall and check the logs daily.
- Monitor your intrusion detection system for possible attacks.
- Limit the information that can be obtained on your organization and the services that are run by your Internet-visible systems.
- Ensure that all patches have been applied for the services that are offered by your system.

(i) What is the best way to minimize possible avenues of attack for your system?

(1/100)

(ii) Explain your answer (by comparing your choice with other steps or policies).

(4/100)

(e) Johnny is worried that someone might be able to intercept and decrypt his VoIP phone calls which is using the standard VoIP protocol: SIP. Thus Johnny considers to use Skype.

(i) What is SIP?

(1/100)

(ii) Why SIP is vulnerable to attacks?

(3/100)

(iii) Why Skype is better used in this situation?

(2/100)

3. (a) Explain the following attacks in term of its definition and example:

(i) Replay Attack.

(2/100)

(ii) Spoofing Attack.

(4/100)

(b) (i) Session hijacking targets the TCP connection between a client and a server. If the attacker learns the initial sequence, he might be able to hijack a connection. Describe in detail on how this occur.

(4/100)

(ii) Describe Domain Name Server (DNS) poisoning and cache poisoning.

(4/100)

(iii) What is ARP Poisoning?

(2/100)

(c) (i) Why is HTML e-mail dangerous?

(2/100)

(ii) Why is an open e-mail relay bad?

(2/100)

(iii) Give **one** (**1**) but the main reason why spam is prevalent today.

(1/100)

(d) The IT department is debating several different e-mail packages, and they ask you to present the security implications of automated malicious code. Briefly explain

- how worms propagate through e-mail, and
- why Microsoft Outlook is such a popular target for worms.

(4/100)

4. (a) You are the security expert of your company. The CIO has tasked your team with the responsibility of designing the corporate network while providing the maximum degree of security. After several discussions to determine the needed network requirements with your team, the following network topology diagram is proposed.

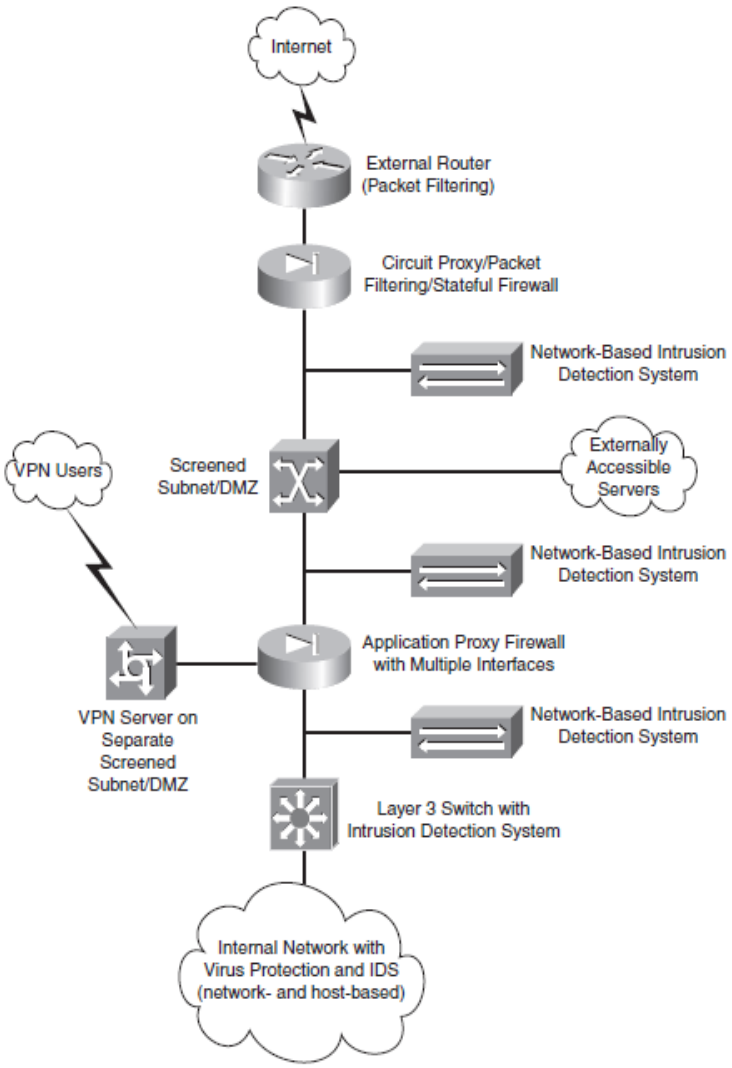


Diagram 1: The proposed network topology

Based on the proposed network topology diagram, explain **HOW** the following security requirements can be done to achieve the most effective solution.

(i) The internal network must be secured against external and internal threats.

(4/100)

(ii) Several servers may be accessed by external users. However, the internal network must be secured, even if these servers are compromised.

(6/100)

(iii) Traveling and home-office users may access the internal network resources.

(5/100)

(iv) Outbound Internet (WWW) access must be screened and filtered.

(2/100)

(b) You are the security analyst for a company that is moving to Web Services as a method of distributed application deployment. Your boss has asked you to write a short report explaining the security issues associated with this new strategy.

Note: Answers to this question will vary, but should explain **two** (**2**) of the ***four types of Web Services vulnerabilities***, and ***how they relate to each other***.

(8/100)

1. (a) Seorang pembangun di syarikat anda yang sedang membangunkan satu aplikasi baru telah bertanya anda sama ada aplikasi berkenaan sepatutnya menggunakan komunikasi berdasarkan TCP atau UDP. Jelaskan kepada beliau kelebihan-kelebihan dan kekurangan-kekurangan setiap protocol berkenaan.

(8/100)

(b) Majikan anda ingin tahu sama ada DHCP sesuai digunakan untuk kedua-dua **persekitaran pelayan** dan **PC**. Nyatakan pandangan anda dan pastikan penerangan diberikan bagaimana DHCP bekerja untuk menyokong pendirian anda.

(6/100)

(c) Syarikat anda, ABC Plastics, adalah satu firma yang membeli resin plastik daripada pengeluar-pengeluar dan menjualnya kepada pengguna-pengguna secara kecil-kecilan. Untuk menjadi lebih berdaya saing, firma ada perlu melakukan perniagaan menerusi Internet, dan oleh kerana itu telah memutuskan untuk menyambungkan rangkaian dalaman syarikat yang terdiri daripada satu pelayan e-mel, satu pelayan fail, dan satu pelayan pangkalan data kepada Internet. Untuk memudahkan pemprosesan urus niaga B2B, satu pelayan sesawang dan satu pelayan aplikasi ditambahkan kepada rangkaian. Syarikat memahami keadaan kritikal yang berkaitan dengan perubahan ini dan telah memulakan satu projek yang diketuai oleh anda untuk mereka bentuk persekitaran baru itu

Gambarkan topologi keselamatan yang bakal anda cadangkan dalam hal ini. Juga, terangkan di mana setiap pelayan sepatutnya ditempatkan dalam rangkaian dan rasional di sebalik keputusan penempatan tersebut.

(7/100)

(d) *Network Address Translation* (NAT) adalah protokol yang boleh digunakan untuk menterjemahkan alamat-alamat IP khusus (*non-routable*) kepada alamat-alamat IP umum (*routable*). Terangkan **dua** (**2**) tujuan perkhidmatan NAT?

(4/100)

2. (a) Anda telah diminta menulis satu polisi keselamatan berkaitan dengan e-mel berasaskan Tanpa Wayar untuk perbadanan anda. Jelaskan dalam polisi berkenaan mengapa anda akan benarkan atau tidak akan benarkan maklumat sulit dihantar menerusi medium ini.

(4/100)

(b) Terdapat pelbagai teknologi yang digunakan oleh peranti-peranti Tanpa Wayar untuk memaksimumkan penggunaan frekuensi-frekuensi radio yang ada. Senaraikan dan terangkan secara ringkas **tiga** (**3**) daripada teknologi berkenaan.

(6/100)

(c) Anda memasang sebuah rangkaian Tanpa Wayar di kediaman anda dan akan melakukan fungsi-fungsi yang berkaitan dengan kerja pada hari-hari di mana anda bertelekomunikasi dari rumah. Senaraikan dan jelaskan secara ringkas dengan contoh yang sesuai **dua** (**2**) langkah-langkah asas yang sepatutnya diambil untuk melindungi rangkaian Tanpa Wayar anda daripada kemungkinan capaian oleh pengguna yang tidak dibenarkan di kompleks kediaman anda.

(4/100)

(d) Pertimbangkan langkah-langkah keselamatan atau polisi-polisi berikut:

- Memasang satu tembok api dan menyemak log setiap hari.
- Memantau sistem pengesan pencerobohan anda untuk sebarang kemungkinan serangan.
- Hadkan maklumat yang boleh diperoleh daripada organisasi anda dan juga perkhidmatan-perkhidmatan yang dilaksanakan oleh sistem-sistem Internet yang boleh dicapai.
- Memastikan semua tampungan-tampungan dibuat ke atas perkhidmatan-perkhidmatan yang ditawarkan oleh sistem anda

(i) Apakah kaedah yang terbaik dalam meminimumkan kemungkinan punca-punca serangan ke atas sistem anda?

(1/100)

(ii) Terangkan jawapan anda (dengan membandingkan pilihan anda dengan langkah-langkah atau polisi-polisi yang lain yang dinyatakan di atas).

(4/100)

(e) Johnny bimbang seseorang mungkin dapat memintas dan mendekripsi panggilan telefon VoIP beliau yang menggunakan protocol piawai VoIP: SIP. Jadi Johnny mempertimbangkan untuk menggunakan Skype.

(i) Apakah SIP?

(1/100)

(ii) Kenapa SIP terdedah kepada serangan?

(3/100)

(iii) Mengapa Skype lebih baik digunakan dalam situasi ini?

(2/100)

3. (a) Jelaskan serangan-serangan berikut dalam bentuk takrifan dan contoh:

(i) Serangan Pengulangan.

(2/100)

(ii) Serangan Perdayaan.

(4/100)

(b) (i) Perampasan Sesi mengarah kepada sambungan TCP antara satu pelanggan dan satu pelayan. Jika penyerang mempelajari jujukan awalan, dia mungkin boleh merampas satu sambungan. Terangkan secara terperinci bagaimana ini boleh berlaku.

(4/100)

(ii) Terangkan peracunan Pelayan Nama Domain (DNS) dan peracunan cache.

(4/100)

(iii) Apakah peracunan ARP?

(2/100)

(c) (i) Kenapa e-mel HTML merbahaya?

(2/100)

(ii) Kenapa sesebuah geganti e-mel terbuka adalah tidak baik?

(2/100)

(iii) Berikan **satu** (**1**) tetapi alasan utama mengapa spam berleluasa hari ini.

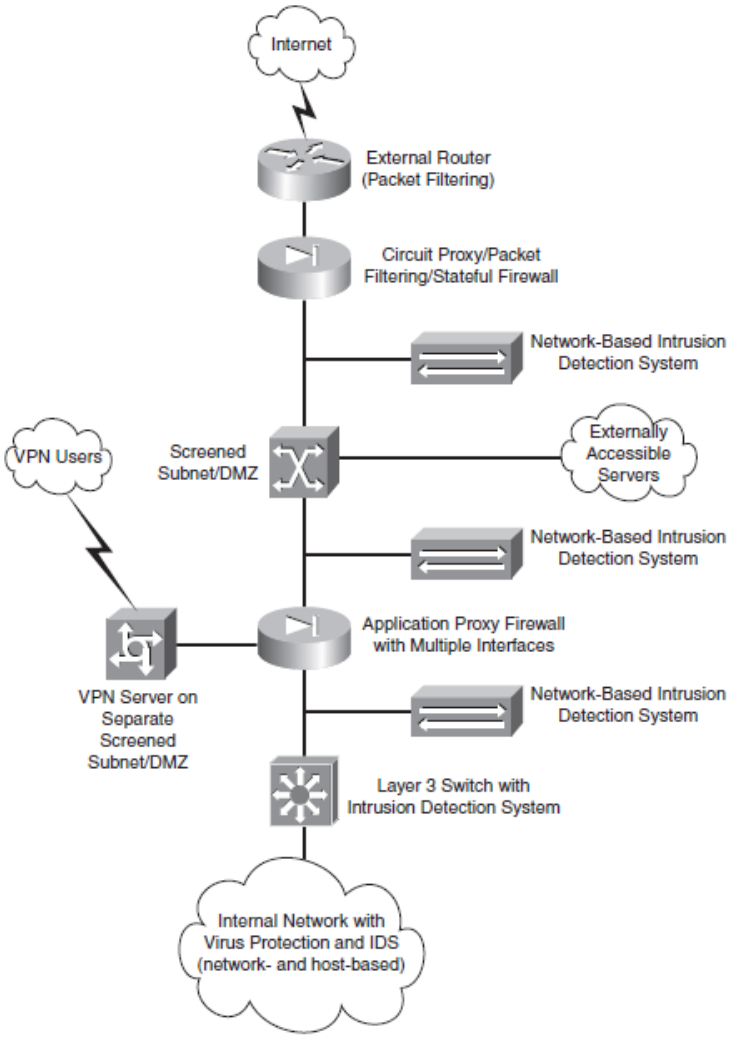
(1/100)

(d) Jabatan IT membahaskan beberapa pakej e-mel yang berbeza, dan mereka meminta anda membentangkan implikasi-implikasi keselamatan kod berniat jahat berautomat. Jelaskan secara ringkas.

- bagaimana cecacing menular menerusi e-mel, dan
- mengapa Microsoft Outlook adalah sasaran popular bagi cecacing.

(4/100)

4. (a) Anda adalah pakar keselamatan syarikat anda. CIO syarikat anda telah menugaskan pasukan anda dengan tanggung jawab merekabentuk sebuah rangkaian korporat dengan sokongan tahap keselamatan yang maksima. Selepas beberapa perbincangan untuk menentukan keperluan-keperluan rangkaian berkenaan bersama pasukan anda, gambar gambar rajah topologi rangkaian berikut dicadangkan.



Gambar rajah 1: Topologi rangkaian yang dicadangkan

Berdasarkan gambar rajah topologi rangkaian yang dicadangkan, jelaskan **BAGAIMANA** keperluan-keperluan keselamatan berikut dapat dilakukan untuk mencapai penyelesaian yang paling berkesan.

(i) Rangkaian dalaman mesti dilindungi daripada ancaman-ancaman luaran dan dalaman.

(4/100)

(ii) Beberapa pelayan boleh dicapai oleh pengguna-pengguna luar. Namun, rangkaian dalaman mesti dilindungi meskipun pelayan-pelayan tersebut dikompromi.

(6/100)

(iii) Pengguna-pengguna yang merantau dan bekerja di rumah boleh mencapai sumber-sumber rangkaian dalaman.

(5/100)

(iv) Capaian keluar Internet (WWW) mesti diskren dan ditapis.

(2/100)

(b) Anda adalah penganalisis keselamatan kepada sebuah syarikat yang sedang memindahkan perkhidmatan-perkhidmatan laman sesawang sebagai satu kaedah untuk mengatur kedudukan aplikasi teragih. Majikan anda meminta anda menulis satu laporan ringkas yang menerangkan isu-isu keselamatan yang berkaitan dengan strategi baru ini.

Nota: Jawapan kepada soalan ini akan berbeza-beza, namun perlu menerangkan **dua** (**2**) daripada ***empat jenis kerentanan perkhidmatan-perkhidmatan sesawang***, dan ***bagaimana ianya berkaitan antara satu sama lain***.

(8/100)