KOLEJ UNIVERSITI TEKNOLOGI TUN HUSSEIN ONN

PEPERIKSAAN AKHIR
SEMESTER I
SESI 2006/2007

NAMA MATA PELAJARAN	:	KESELAMATAN RANGKAIAN
KOD MATA PELAJARAN	:	BTI 4743
KURSUS	:	4 BTI
TARIKH PEPERIKSAAN	:	NOVEMBER 2006
JANGKA MASA	:	3 JAM
ARAHAN	:	JAWAB **EMPAT(4)** DARIPADA LIMA(5) SOALAN

KERTAS SOALAN INI MENGANDUNGI 8 MUKA SURAT

Q1 (a) Jemal Sultaninov, a professional attacker, usually begins a thorough research before attacking his target. He picks up a lot of essential information during this phase. In at least **FIVE (5)** steps, describe possible activities Jemal might be involved in, during this phase. Please include example of *tools* he may use at each of the step.

(15 marks)

(b) Once sufficient information has been obtained by a hacker, there are only few more steps left to compromise a system. Describe **FIVE (5)** continuing steps that would make him deeply compromise a system.

(10 marks)

Q2 (a) Assuming you are auditing a university's network. Predict the extend of damage it could caused by the following state of practice in the university. Consider the following findings during your audit:

(i) Sontoroyo, an administrative staff, downloads and installed many programs from Internet, regardless from trusted or untrusted sites. He also installs some pirated games.

(5 marks)

(ii) The hype in Wireless Technology has prompt the Pusat Teknologi Maklumat to go wireless. Many access points have been install around the campus, including in the library and cafeterias. To achieve security and easy management, a staff responsible to install the wireless access points has decided to use similar WEP for all access points. No other mechanisms are used to control access to the APs, except the WEP.

(5 marks)

(b) Offline attack is extremely hard to detect because the attacker gets to a target machine and copy whatever he needs, and then immediately leave the machine. Describe **THREE (3)** possible types of files that he may have copied, and how shall he proceed with what he has?

(9 marks)

(c) Mat Kemin Syamion, a Mummy Commercial Bank customer, who knows some hacking techniques, has decided to hack his own account at mummybank.com. To his amazement, he figured out that some of the techniques really work to crack his own account. He informed the bank that he has found some weaknesses in mummybank.com, and he is worried that his account is not secure anymore, and he happily offers a paid service to do more comprehensive testing and suggest appropriate countermeasures to strengthen mummybank.com. Do you think his action is appropriate? Discuss also the consequence of his act.

(6 marks)

Q3 (a) After graduation, Muadz successfully obtained a new job as IT officer in a private organization in Kuala Lumpur. After some investigation, he started to realize that the organization does not have any plan or program handling on security issues. Describe **THREE (3)** information security goals that he should always try to achieve in order to secure the organization's network.

(9 marks)

(b) Each link in your security system is important. Why do we need to be so comprehensive?

(6 marks)

(c) As proven by the case of Kevin Mitcnick, having all security mechanisms such as Firewall, Intrusion Detection Systems, regularly updated corporate antivirus, strong password, update patch management, host hardening, etc does not guarantee a perfect security system. He can simply bypass all those security mechanism.

(i) Using what technique, he managed to bypass all those security mechanisms? Provide one example on how such technique can be applied.

(5 marks)

(ii) How to prepare an organization from such kind of attack?

(5 marks)

Q4 (a) Security staff should not assume that all staffs know how to properly construct their password. Each staff must be trained on the concept of strong password. Describe in detail all the characteristics of strong password together with appropriate examples and explain how each of those characteristics will make password cracking harder.

(10 marks)

(b) Password is one of the most favorite targets for an attacker and the fact is that, all passwords can be cracked. Describe **THREE (3)** techniques how passwords can be cracked.

(9 marks)

(c) Why would a network administrator crack passwords on his own server?

(6 marks)

Q5 (a) Knowing the types of attacker working behind your network is important so that appropriate security measures can be prepared to contain their malicious activities.

(i) Compare the different types of attackers in terms of their motivation, methodology, technical knowledge, and likely damage they could do to a network system.

(9 marks)

(ii) Explain how to protect your organization from each type of attackers.

(3 marks)

(b) Propose suitable firewall topology (network diagram) for each of the following customer:

Customer A: 5 students living in the same house accessing broadband service from TMNET Streamyx. Lower cost is important. No servers, mainly for browsing.

Customer B: A medium sized organization with more than 100 network nodes. Staff will be able to access Internet. It has fixed IPs assigned to DNS, Web Server, Proxy Server and email server.

(8 marks)

(c) Is hardware box firewall stronger than software firewall? Provide **TWO (2)** reasons to support your answer.

(5 marks)

S1 (a) Jemal Sultaninov, seorang penggodam profesional, selalunya memulakan tugasnya dengan membuat kajian terperinci sebelum menyerang mangsanya. Dia akan mendapatkan banyak maklumat penting semasa fasa ini. Dalam sekurang-kurangnya **LIMA (5)** langkah, terangkan aktiviti-aktiviti yang boleh dilakukan oleh Jemal semasa bekerja pada fasa ini. Senaraikan *peralatan* yang mungkin beliau gunakan pada setiap langkah yang diberikan.

(15 markah)

(b) Apabila maklumat yang mencukupi telah diperolehi oleh seseorang penggodam, hanya tinggal beberapa langkah sahaja lagi sebelum sistem yang ingin diserang itu dapat dikuasai. Terangkan **LIMA (5)** langkah seterusnya yang membolehkan penggodam menguasai sepenuhnya sesebuah sistem.

(10 markah)

S2 (a) Katakan kamu telah dipanggil untuk mengaudit sebuah rangkaian universiti daripada aspek keselamatan. Ramalkan sejauh mana kerosakan-kerosakan yang boleh diakibatkan daripada pengamalan perkara-perkara berikut:

(i) Sontoroyo, seorang staf pentadbiran, sentiasa memuat-turun program-program daripada Internet, tanpa mengira samada ia daripada laman yang boleh dipercayai atau pun tidak. Dia juga memasang beberapa permainan yang dibelinya dengan harga yang sangat murah daripada Imby Plaza (cetak rompak).

(5 markah)

(ii) Perkembangan teknologi tanpa wayar yang amat pesat dan memberangsangkan telah menyebabkan Pusat Teknologi Maklumat membuat keputusan untuk menjadikan kampus universiti boleh diakses tanpa wayar. Banyak *access points* (AP) telah di pasang diseluruh kampus, termasuklah di perpustakaan dan kafetaria. Untuk tujuan keselamatan dan memudahkan pengurusan AP, staf yang bertanggungjawab kepada pemasangan tersebut telah memutuskan untuk menggunakan WEP yang sama untuk semua AP. Tiada mekanisma lain lagi digunakan untuk mengawal akses ke AP-AP tersebut melainkan WEP.

(5 markah)

(b) Serangan *offline* adalah sangat sukar untuk dikesan kerana penyerang akan pergi kepada PC mangsanya dan menyalin apa-apa yang ia kehendaki, dan kemudian dengan segera berlalu daripada situ. Terangkan **TIGA (3)** jenis fail yang diperolehinya itu dan bagaimana seterusnya dia menggunakan fail-fail tersebut untuk melancarkan serangan.

(9 markah)

(c) Mat Kemin Syamion, seorang pelanggan Bank Komersial Mummy, yang mengetahui beberapa cara menggodam, telah membuat keputusan untuk menggodam akaunnya sendiri bagi mengukur tahap keselamatan akaunnya di mummybank.com. Tanpa diduga, beberapa teknik yang digunakannya telah dapat menggodam akaunnya. Dengan rasa penuh tanggungjawab, dia telah memberitahu bank tersebut akan kelemahan yang ditemuinya di mummybank.com. Dia juga risau akan keselamatan akaunnya. Oleh itu, dia dengan tulus hati memberi tawaran berpatutan kepada bank muamalat untuk melakukan pengujian yang lebih lengkap lagi dan mencadangkan beberapa penyelesaian untuk menguatkan mummybank.com.

Berikan pandangan anda tentang perbuatan Mat Kemin. Bincangkan juga kesan daripada tindakannya itu.

(6 markah)

S3 (a) Selepas bergraduat, Muadz berjaya mendapatkan satu pekerjaan baru sebagai pegawai teknologi maklumat di sebuah organisasi swasta di Kuala Lumpur. Selepas melakukan sedikit penyiasatan, dia mendapati organisasi itu tidak mempunyai perancangan atau program keselamatan maklumat. Terangkan **TIGA (3)** matlamat keselamatan maklumat yang perlu beliau capai supaya rangkaian organisasi menjadi lebih selamat.

(9 markah)

(b) Setiap bahagian atau sambungan dalam sistem keselamatan kamu adalah penting. Kenapa kita perlu bersikap komprehensif dalam menangani keselamatan?

(6 markah)

(c) Seperti yang telah dibuktikan oleh kes Kevin Mitcnick, mempunyai semua mekanisma seperti *Firewall*, *IDS*, antivirus terkini, katakunci yang kuat, pengurusan *patch* yang baik, menguatkan hos dan lain-lain lagi, tidak memberi jaminan bahawa sistem kita bebas daripada masalah. Kevin telah memintas semua mekanisme itu.

(i) Menggunakan teknik apakah dia telah berjaya melepasi semua mekanisma-mekanisma tadi? Berikan satu contoh bagaimana melakukan teknik tersebut.

(5 markah)

(ii) Bagaimana kita menyediakan sesebuah organisasi daripada diserang melalui teknik yang anda bincangkan diatas.

(5 markah)

S4 (a) Staf keselamatan tidak boleh menganggap semua stafnya tahu bagaimana membina sebuah password yang betul. Setiap staf perlu dilatih mengenai konsep katakunci kuat. Bincangkan semua ciri-ciri katakunci yang kuat berserta dengan contoh-contohnya yang sesuai, serta terangkan bagaimana setiap ciri itu dapat menyusahkan proses *cracking* katakunci.

(10 markah)

(b) Katakunci adalah salah satu tumpuan penggodam dan secara faktanya semua katakunci boleh di*crack*. Terangkan **TIGA (3)** teknik bagaimana katakunci dapat di *crack* kan.

(9 markah)

(c) Pada ketika-ketika tertentu, kenapa seorang pentadbir rangkaian perlu *crack* katakunci di pelayannya sendiri?

(6 markah)

S5 (a) Mengetahui pelbagai jenis penyerang yang mungkin sedang menggodam rangkaian anda adalah amat penting supaya penyelesaian-penyelesaian tertentu boleh disediakan bagi menghadapi serangan-serangan mereka.

(i) Bandingkan pelbagai jenis penyerang dari aspek motivasi, metodologi, pengetahuan teknikal dan sejauh mana kerosakan yang boleh mereka akibatkan.

(9 markah)

(ii) Terangkan bagaimana melindungi organisasi anda daripada setiap jenis penyerang.

(3 markah)

(b) Cadangkan sebuah topologi *firewall* (lakarkan diagram rangkaian) untuk setiap pelanggan berikut:

Pelanggan A: 5 pelajar yang tinggal dirumah yang sama, menerima servis jalurlebar Internet daripada tmnet Streamyx. Kos pemasangan dan penyelenggaraan amat rendah. Tiada pelayan, hanya untuk melayari Internet sahaja.

Pelanggan B: Sebuah organisasi bersaiz sederhana dengan mempunyai lebih 100 nod rangkaian. Semua staf boleh mengakses Internet. Ia mempunyai alamat IP tetap yang telah diletakkan pada pelayan-pelayan DNS, Web, Proxy dan juga email.

(8 markah)

(c) Adakah *firewall* peranti keras lebih kuat berbanding *firewall* peranti lembut? Berikan 2 sebab untuk menyokong pandangan anda.

(5 markah)