UU KK 2013

NASKAH UJIAN INI TERDIRI DARI 80 SOAL PILIHAN GANDA

SETIAP SOAL PILIHAN GANDA HANYA ADA SATU JAWABAN YANG BENAR. PILIHLAH SATU DARI EMPAT JAWABAN YANG ADA. HITAMKAN LINGKARAN PADA LEMBAR JAWABAN SESUAI PILIHAN SAUDARA.

1. Pada aplikasi bisnis yang menjadi target oleh seorang hacker melakukan kejahatan komputer adalah :
   A. On-line banking
   B. e-commerce
   C. Jawaban A dan B benar
   D. Jawaban A dan B salah

2. Sistem informasi yang dirancang untuk pengamanan disebabkan beberapa hal, ***kecuali***:
   A. Ditemukan lubang keamanan
   B. Kesalahan konfigurasi
   C. Penyadapan
   D. Penambahan perangkat baru

3. Mengapa keamanan komputer sangat dibutuhkan :
   A. Karena adanya *"Information-Based Society"* yang menyebabkan nilai informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akuratmenjadi sangat esensial bagi sebuah organisasi.
   B. Karena adanya infrastruktur jaringan computer seperti LAN dan internet, memungkinkan menyediakan informasi secara cepat.
   C. Jawaban A dan B benar
   D. Jawaban A dan B salah

4. Seorang criminal (Hacker) berusaha pura-pura sebagai orang yang berhak mengakses informasi, teknik ini dikenal dengan istilah :
   A. Social engineering
   B. Computer engineering
   C. Jawaban A dan B salah
   D. Jawaban A dan B benar

5. Di bawah ini alasan mengapa kejahatan computer semakin meningkat, ***kecuali*** :
   A. Sentralisasi server.
   B. Meningkatnya aplikasi bisnis dalam bidang IT dan jaringan komputer.
   C. Kemampuan pemakai semakin meningkat.
   D. Desentralisasi server.

6. Menurut David Icove [John D. Howard, *"An Analysis Of Security Incidents On The Internet 1989 - 1995,"* PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 1997.] berdasarkan lubang keamanan, keamanan dapat diklasifikasikan, ***kecuali*** :
   A. Keamanan yang bersifat fisik
   B. Keamanan Keamanan yang berhubungan dengan orang (personel).
   C. Keamanan Jaringan.
   D. Keamanan dari data dan media serta teknik komunikasi *(communications)*.

7. *Denial of service*, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlah pesan). Merupakan contoh dari keamanan :
   A. Keamanan yang bersifat fisik
   B. Keamanan Keamanan yang berhubungan dengan orang (personel).
   C. Keamanan Jaringan.
   D. Keamanan dari data dan media serta teknik komunikasi *(communications)*

8. Di bawah ini aspek-aspek keamanan komputer, ***kecuali*** :
   A. Modification.
   B. Authentication
   C. Integrity.
   D. Privacy

9. Sebuah usaha untuk melumpuhkan sistem yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan servis-servisnya disebut :
   A. Sniffer
   B. Land attack
   C. Latierra
   D. Denial of service attack

10. Metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, adalah aspek keamanan :
   A. Modification.
   B. Authentication
   C. Integrity.
   D. Privacy

11. Di bawah ini model serangan pada keamanan, adalah :
   A. Modification.
   B. Authentication
   C. Integrity.
   D. Privacy

12. Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site, adalah model serangan :
   A. Modification.
   B. Authentication
   C. Interception
   D. Privacy

13. Penyadapan *(wiretapping)* adalah contoh serangan :
   A. Modification.
   B. Authentication
   C. Interception
   D. Interupption

14. Ilmu dan seni untuk menjaga pesan agar aman adalah :
   A. Kriptografi
   B. Cryptanalyst
   C. Cryptanalysis
   D. Cryptographers

15. Istilah-istilah berikut yang terdapat pada kriptografi, ***kecuali*** :
   A. Plaintext
   B. Digitaltext
   C. Enkripsi
   D. Dekripsi

16. Seni dan ilmu untuk memecahkan *ciphertext* tanpa bantuan kunci, adalah :
A. Kriptografi
B. Cryptanalyst
C. Cryptanalysis
D. Cryptographers

17. Metode substitution cipher secara Caesar cipher adalah :
A. Setiap huruf diganti dengan huruf yang berada tiga posisi dalam urutan alfabet dengan huruf kecil
B. Setiap huruf diganti dengan huruf yang berada lima posisi dalam urutan alfabet dengan huruf kecil
C. Setiap huruf diganti dengan huruf yang berada tiga posisi dalam urutan alfabet dengan huruf besar
D. Setiap huruf diganti dengan huruf yang berada lima posisi dalam urutan alfabet dengan huruf besar

18. Rencana strategis, formula-formula produk, database pelanggan/karyawan dan database operasional, adalah salah satu contoh aplikasi enkripsi :
A. Militer dan pemerintahan.
B. Jasa Telekomunikasi
C. Data perbankan
D. Data Konfidensial perusahaan

19. Suatu kombinasi dari peragkat lunak dan perangkat keras yang dirancang untuk memeriksa aliran trafik jaringan dan permintaan servis disebut :
A. Proxy
B. Firewall
C. Router
D. Gateway

20. Pencipta program dapat menyebarkan ke pemakai-pemakai dengan menempatkan program di direktori bersama dan menamai programnya sedemikian rupa sehingga disangka sebagai program utilitas yang berguna, merupakan program dari :
A. Logic bomb.
B. Bacteria.
C. Trapdoor.
D. Trojan horse.

21. Perangkat pembantu otomatis yang dapat menguji keamanan yang dikelola disebut :
A. Automated Pack
B. Automated Service
C. Automated tools
D. Automated Help

22. Jika seseorang bisa merekam pesan-pesan *handshake* (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak, adalah jenis penyerangan :
A. Man-in-the-middle
B. Chosen-plaintext attack
C. Replay attack
D. Chosen-key attack

23. Bermutasi setiap kali melakukan infeksi merupakan klasifikasi virus :
A. Parasitic virus.
B. Polymorphic virus
C. Memory resident virus
D. Stealth virus.

24. Viruses, worms, trojan horses, logic bomb adalah contoh-contoh serangan sistem komputer jenis :
A. Errors and omissions
B. Employee sabotage
C. Malicious hackers (crackers)
D. Malicious code

25. Cara untuk mengamankan file yang dilakukan di luar komputer adalah :
A. Backup ke jaringan
B. Mengganti nama file
C. Tidak disimpan
D. Menggunakan password

26. Proses penentuan identitas dari seseorang yang sebenarnya, hal ini diperlukan untuk menjaga keutuhan (integrity) dan keamanan (security) data, pada proses ini seseorang harus dibuktikan siapa dirinya sebelum menggunakan layanan akses, adalah jenis pembatasan akses jaringan :
A. Membuat tingkatan akses
B. Mekanisme kendali akses
C. Sistem otentifikasi user
D. Pembuatan firewall

27. Virus yang menginfeksi master boot record atau boot record dan menyebar saat sistem diboot dari disk yang berisi virus disebut :
A. Boot sector virus
B. Parasitic virus
C. Polymorphic virus
D. Stealth virus

28. Upaya mengamankan proteksi password dengan cara menambahkan string pendek ke string password yang diberikan pemakai sehingga mencapai panjang password tertentu dikenal dengan istilah :
A. Otoritas password
B. Variasi password
C. One time password
D. Salting

29. Kebijaksanaan dari konfigurasi firewall yang tidak diperbolehkan secara eksplisit dianggap tidak diperbolehkan disebut :
A. Protection
B. Probe service
C. Prohibitted
D. Permitted

30. Salah satu kemampuan firewall yang dikenal dengan istilah privilege limitation, yaitu...
A. Memperbolehkan orang luar untuk mengakses informasi yang tersedia dalam salah satu computer dalam jaringan kita.
B. Membatasi para user jaringan sesuai dengan otorisasi atau hak-hak yang diberikan kepadanya.
C. Membatasi para user dalam jaringan untuk mengakses ke alamat-alamat tertentu di luar jangkauan kita.
D. Mengakibatkan IP address dalam jaringan ditransalasikan ke suatu IP address yang baru.

31. Salah satu tipe firewall yang melakukan control akses ke dalam maupun ke luar jaringan dikenal dengan istilah :
A. Personal firewalls
B. Application/proxy firewalls
C. Packet filtering firewalls
D. Internet firewall

32. Firewall yang tergantung OS, adalah :
A. Sunscreen
B. Gauntlet
C. Bigfire
D. Cyberguard

33. Berikut hal-hal yang menyebabkan file dapat hilang, ***kecuali*** :
A. Masalah hardware
B. Virus
C. Media penyimpanan yang besar
D. Masalah software

34. Bagaimana cara mengamankan file pada komputer ?
A. Menggunakan password
B. Pencegahan virus
C. Pembatasan hak akses
D. Benar semua

35. Algoritma yang menggunakan kunci sama untuk proses enkripsi dan dekripsi yaitu algoritma :
A. Algoritma Simetris
B. Algoritma Block Cipher
C. Algoritma Stream Cipher
D. Algoritma Asimetris

36. Jika *spoofing* terkadang hanya menipu satu pihak, maka dalam skenario ini, saat Anto hendak berkomunikasi dengan Badu, Maman di mata Anto seolah-olah adalah Badu, dan Maman dapat pula menipu Badu sehingga Maman seolah-olah adalah Anto. Maman dapat berkuasa penuh atas jalur komunikas ini, dan bisa membuat berita fitnah. Ini merupakan jenis penyerangan :
   A. Man-in-the-middle
   B. Chosen-plaintext attack
   C. Replay attack
   D. Chosen-key attack

37. Setiap huruf digantikan dengan huruf yang berada tiga (3) posisi dalam urutan alfabet adalah metode :
   A. Caesar Cipher
   B. Vigenere
   C. ROT13
   D. Semua salah

38. Enkripsi untuk mengamankan informasi konfidensial baik berupa suara, data, maupun gambar yang akan dikirimkan ke lawan bicaranya, adalah contoh aplikasi enkripsi pada pengamanan :
   A. Militer dan pemerintahan.
   B. Jasa Telekomunikasi
   C. Data perbankan
   D. Data Konfidensial perusahaan.

39. Di bawah ini jenis penyerangan pada protocol adalah :
   A. Sniffing
   B. Chosen-plaintext attack
   C. Replay attack
   D. Spoofing

40. Pada penyerangan ini, cryptanalyst tidak hanya memiliki akses atas ciphertext dan plaintext untuk beberapa pesan, tetapi ia juga dapat memilih plaintext yang dienkripsi, adalah jenis penyerangan :
   A. Known-plaintext attack
   B. Chosen-plaintext attack
   C. Replay attack
   D. Spoofing

41. Di bawah ini jenis penyerangan pada jalur komunikasi, adalah :
   A. Known-plaintext attack
   B. Chosen-plaintext attack
   C. Replay attack
   D. Chosen-key attack

42. Program yang mengkonsumsi sumber daya sistem dengan mereplikasi dirinya sendiri merupakan program jahat :
   A. Logic bomb.
   B. Bacteria
   C. Trapdoor
   D. Trojan horse.

43. Siklus hidup virus terdapat empat fase. Fase dimana Virus menempatkan kopian dirinya ke program lain atau daerah sistem tertentu di disk disebut fase :
   A. Fase Tidur
   B. Fase Propagasi
   C. Fase Pemicuan
   D. Fase Eksekusi

44. Virus yang bentuknya telah dirancang agar dapat menyembunyikan diri dari deteksi perangkat lunak antivirus, merupakan klasifikasi virus :
   A. Parasitic virus.
   B. Polymorphic virus
   C. Memory resident virus.
   D. Stealth virus.

45. Di bawah ini merupakan pembatasan akses ke jaringan pada sistem keamanan jaringan, ***kecuali*** :
   A. Membuat tingkatan akses.
   B. Mekanisme kendali akses.
   C. Sistem Otentikasi User
   D. Pembuatan firewall

46. Berikut ini yang ***bukan*** merupakan teknik pemulihan adalah :
A. Defered Update
B. Manager Pemulihan
C. Immediate Update
D. Shadow Paging

47. Teknik pemulihan yang menggunakan page bayangan dimana pada prosesnya terdiri dari 2 tabel yang sama, yang satu menjadi tabel transaksi dan yang lain digunakan sebagai cadangan disebut teknik :
A. Defered Update
B. Manager Pemulihan
C. Immediate Update
D. Shadow Paging

48. Perubahan pada DB akan segera tanpa harus menunggu sebuah transaksi tersebut disetujui merupakan teknik :
A. Defered Update
B. Immediate Update
C. Manager Pemulihan
D. Shadow Paging

49. Di bawah ini merupakan tingkatan keamanan pada database, ***kecuali*** :
A. Fisikal
B. Sistem Operasi
C. Manusia
D. Semua salah

50. Metode pembatasan bagi pengguna untuk mendapatkan model database yang sesuai dengan kebutuhan perorangan adalah :
A. Otorisasi.
B. Tabel View.
C. Backup and Restore
D. Kesatuan data.

51. Perintah pada SQL yang digunakan untuk mencabut wewenang yang dimiliki oleh pemakai, adalah :
A. Revoke
B. Insert
C. Grant
D. Update

52. Di bawah ini arsitektur keamanan pada system Linux, adalah :
A. Administrasi user dan group
B. Keamanan system file
C. Kontrol akses secara diskresi
D. Semua benar

53. Prosedur dari Sistem Operasi atau aplikasi merekam setiap kejadian dan menyimpan rekaman tersebut untuk dapat dianalisa, adalah :
A. Intrusion Detection.
B. Logging.
C. Enkripsi
D. Kontrol akses jaringan.

54. Sejenis komersial email yang menjadi sampah mail (junkmail), adalah :
A. Worms
B. Virus
C. Spam
D. Spyware

55. Suatu program dengan tujuan menyusupi iklan tertentu (adware) atau mengambil informasi penting di komputer pengguna, adalah :
A. Worms
B. Virus
C. Spam
D. Spyware

56. Di bawah ini merupakan tips untuk keamanan komputer, ***kecuali*** :
A. Hindari booting dari floopy disk
B. Backup data secara regular
C. Gunakan software antivirus
D. Salah semua

57. Di bawah ini kelemahan dari firewall, adalah :
A. Firewall dapat digunakan untuk membatasi pengunaan sumberdaya informasi
B. Firewall tidak dapat melindungi dari serangan dengan metoda baru yang belum dikenal oleh Firewall.
C. Jawaban A dan B benar
D. Jawaban A dan B salah

58. Firewall yang menggunakan dua screening-router dan jaringan tengah (*perimeter network*) antara kedua router tersebut, di mana ditempatkan bastion host, adalah arsitektur firewall :
A. Screened subnet (SSG)
B. Screened-host (SHG)
C. Dual-homed host (DHG)
D. Salah semua

59. Ancaman terhadap availability yaitu data dan informasi yang berada dalam system computer dirusak atau dibuang, sehingga menjadi tidak ada dan tidak berguna, dikenal dengan istilah :
A. Interruption
B. Modification
C. Interception
D. Fabrication

60. Suatu tipe dari IPsec yang berhubungan dengan penggunaan untuk paket enkripsi dan autentikasi adalah :
A. AH
B. ESP
C. SA
D. SPI

61. Network monitoring dapat digunakan untuk mengetahui adanya lubang keamanan. Contoh-contoh program network monitoring antara lain :
A. SNMP collector
B. WebXRay
C. SNMP trap
D. Honeypot

62. Personal encryption kriptografi yang memanfaatkan public key cryptography untuk proses enkripsi dan digital signing terhadap file-file umum seperti email adalah.:
A. DES
B. IDEA
C. PGP
D. RSA

63. Piranti tambahan yang digunakan dalam sebuah jaringan dengan tujuan untuk memperoleh keamanan jaringan yaitu :
A. Switch
B. Hub
C. Router
D. Firewall

64. Tujuan akhir dari perancangan sistem keamanan komputer adalah :
A. Integrity, availability, telecomunication
B. Integrity, availability, confidentiality
C. Hardware, software, firmware
D. Database, operating system, telecomunication

65. Seluruh hubungan/kegiatan dari dalam ke luar harus melawati firewall, merupakan :
A. Karakteristik firewall
B. Teknik firewall
C. Layanan firewall
D. Segment

66. Yang disebut segmen pada perlindungan yang menggunakan firewall yaitu :
A. Client
B. LAN
C. Server
D. Benar semua

67. Aset-aset perusahaan yang dilindungi dalam sistem keamanan komputer adalah :
A. Hardware, software, firmware, information/data, telecommunications
B. Hardware, software, operating system, data, network
C. Hardware, software, information, management, operational
D. Hardware, software, operating system, data, access

68. Yang ***bukan*** merupakan fungsi pendukung (Function Support) dalam sistem keamanan komputer adalah :
A. Technology provider
B. Disaster Contigency and Recovery Plan
C. Quality assurance
D. Training management

69. Pengguna diperbolehkan menambah data baru, tetapi tidak dapat memodifikasi data yang sudah ada, adalah :
A. Read Authorization
B. Insert Authorization
C. Index Authorization
D. Update Authorization

70. Teknik kriptografi dengan memindahkan atau merotasi karakter dengan aturan tertentu :
A. Subtitusi
B. Permutasi
C. Ekspansi
D. Blocking

71. Meletakkan huruf konsonan atau bilangan ganjil yang menjadi awal dari suatu kata di akhir kata itu dan menambahkan akhiran "an". Bila suatu kata dimulai dengan huruf vokal atau bilangan genap, ditambahkan akhiran "i" ini merupakan salah satu contoh dari teknik kriptografi :
A. Subtitusi
B. Permutasi
C. Ekspansi
D. Blocking

72. Di bawah ini adalah fungsi firewall Linux, ***kecuali*** :
A. Analisa dan filtering paket
B. Blocking content dan protocol
C. Autentikasi koneksi dan enkripsi
D. Semua jawaban salah

73. Prosedur dari sistem operasi atau aplikasi merekam setiap kejadian dan menyimpan rekaman tersebut untuk dapat dianalisa, pada Linux disebut :
A. Network access control
B. Logging
C. Enkripsi
D. User account

74. Di bawah ini contoh-contoh produk otentikasi user, ***kecuali*** :
A. Secureid ACE (Access Control Encryption)
B. One time password
C. Password Authentication Protocol (PAP)
D. Terminal Access Controller Access Control System (TACACS)

75. System token hardware seperti kartu kredit berdisplay, pemakai akan menginput nomor pin yang diketahui bersama, lalu memasukkan pascode bahwa dia pemilik token adalah :
A. Secureid ACE (Access Control Encryption)
B. One time password
C. Password Authentication Protocol (PAP)
D. Terminal Access Controller Access Control System (TACACS)

76. Sistem pemantau jaringan (network monitoring) dapat digunakan untuk :
A. Memantau apakah jaringan aman.
B. Tambahan keamanan jaringan
C. Mengetahui adanya lubang keamanan
D. Mengetahui adanya penyusup

77. Metode pembatasan bagi pengguna untuk mendapatkan model database yang sesuai dengan kebutuhan perorangan. Metode ini dapat menyembunyikan data yang tidak digunakan atau tidak perlu dilihat oleh pengguna, adalah :
A. Otorisasi
B. Backup
C. Recovery
D. Tabel view

78. Proses secara periodik untuk mebuat duplikat dari database dan melakukan logging file (atau program) ke media penyimpanan eksternal adalah :
A. Otorisasi
B. Backup
C. Recovery
D. Tabel view

79. Pada database relasional untuk pengamanan dapat dilakukan beberapa level, ***kecuali*** :
A. Read Authorization
B. Insert Authorization
C. Index Authorization
D. Update Authorization

80. Ada beberapa otorisasi tambahan untuk memodifikasi data, yaitu :
A. Read Authorization
B. nsert Authorization
C. Index Authorization
D. Update Authorization