DIKLAT
HMIF

2018

KRIPTOGRAFI

AIK21424

PILIHAN

DAFTAR ISI

UJIAN TENGAH SEMESTER 2013/2014

Ujian Tengah Semester Genap 2013/2014
Jurusan Ilmu Komputer/Informatika
FSM Universitas Diponegoro Semarang

Mata Kuliah	: Kemanan Jaringan	Hari/ Tanggal	: Senin, 21 April 2014
Beban	: 3 SKS	Jam	: 13.00 – 14.10 WIB
Dosen	: -Sutikno, ST, M.Cs	Waktu	: 75 Menit
	-Indra Waspada, ST, MTI	Sifat	: Buku tertutup

Perhatian: Segala bentuk **KECURANGAN** (mencontek teman, memberi contekan, mencontek catatan, kerja sama dan sejenisnya) akan diberikan nilai **0 (NOL)**.

Jawablah Pertanyaan dibawah ini dengan singkat dan jelas ?

1. Sebutkan 4 alasan utama mengapa informasi harus diamankan?
2. Sebutkan 2 hal yang dilakukan virus setelah menginfeksi computer?
3. Bagaimana langkah-langkah serangan dengan menggunakan *Cross Site Scripting* (XSS) dan bagaimana cara melakukan pertahanannya (sebutkan 2 cara)?
4. Sebutkan kerentanan-kerentanan keamanan dalam menggunakan *Instant Messaging* (IM) dan sebutkan cara mengamankanya (masing-masing sebutkan 2) ?
5. Apa hasil dari algoritma *transposition ciper* dengan plaintext "SAYA AKAN DATANG DUA MINGGU LAGI" jika digunakan kunci dan nilai angka sebagai berikut:

I	L	K	O	M
1	3	2	5	4

6. Apa yang disebut dengan *Public Key Infrastructure* (PKI) dan sebutkan 4 komponen dalam PKI tersebut?

UJIAN AKHIR SEMESTER 2013/2014

Mata Kuliah	: Keamanan Jaringan	Dosen	: - Sutikno, ST, MCs.
Beban	: 3 SKS		- Indra Waspada, ST, MTI
Semester	: 3	Hari/ Tanggal	: Senin/ 7 Juli 2014
Sifat	: close book	Waktu	: 100 menit

Gunakan alat tulis sendiri. Mencontek, komunikasi antarpeserta, atau peminjaman barang berarti kecurangan (Nilai = 0).

I. Kerjakanlah pada lembar jawaban yang telah disediakan bersama soal ini.

1) A(n) _____ is an account that is secretly set up without the administrator's knowledge or permission that allows for remote access to the device.
   a) back door
   b) User Installation Account (UIA)
   c) privilege account
   d) default account

2) A(n) _____ attack attempts to consume network resources so that the devices cannot respond to legitimate requests
   a) System overflow
   b) reverse ping
   c) Denial of service
   d) ARP spoofing

3) The difference between a replay attack and a man-in-the-middle attack is _____.
   a) replay attacks are always faster
   b) man-in-the-middle attack can be prevented yet a replay attack cannot
   c) replay attacks sends the transmission immediately
   d) replay attack makes a copy of the transmission before sending it to the recipient

4) Where is the physical address and IP address mappings stored?
   a) On the Domain Name System(DNS) server
   b) In a local hosts file
   c) In the ARP cache
   d) On a network file server

5) In a(n) _____ attack the attacker overflows a switch's address table with fake media access control (MAC) addresses and makes the switch act like a hub, sending packets to all devices.
   a) Address Domain Resolution (ADR)
   b) switch flooding
   c) MAC ARP impersonation
   d) switch advertisement

6) A back door can be created by each of the following **except** _____.
   a) a spyware
   b) a virus
   c) a Trojan horse
   d) a programmer of the software on the device

7) Using _____, an attacker convince the authentic DNS server to accept fraudulent DNS entries sent from attacker's DNS server.
   a) DNS spoofing
   b) zone transfer imaging (ZTI)
   c) DNS transfer
   d) name resolution spoofing

8) Which of the following could not be the result of an ARP poisoning attack?
   a) Steal data intended for another device
   b) Force a switch to revert to a hub
   c) Change entries in a DNS zone transfer table
   d) Prevent Internet access to users on a network

9) A virtual LAN (VLAN) allows devices to be grouped ___.
   a) based on subnets
   b) only around core switches
   c) logically
   d) directly to routers

10) Convergence combines voice, data, and video traffic __.
   a) through hubs
   b) over a single IP network
   c) one stream at a time
   d) only on wireless networks

11) Each of the following is a convergence security vulnerability except _____.
   a) convergence resource attacks (CRA)
   b) VoIP protocols
   c) spam
   d) lack of encryption

12) Which of the following is **not true** regarding a demilitarized zone (DMZ)?
   a) It contains servers that are only used by internal network users
   b) It typically has an e-mail or Web server
   c) It can be configured to have one or two firewalls
   d) provides an extra degree of security

13) Network address translation (NAT) ___
   a) substitutes MAC addresses for IP addresses
   b) can only be found on core routers
   c) can be stateful or stateless
   d) substitutes local IP addresses for public IP addresses

14) Another name for a packet filter is a(n) _____.
   a) DMZ
   b) firewall
   c) proxy server
   d) honeypot

15) The _____ establishes the action that a firewall takes on a packet.
   a) host cache
   b) rule base
   c) syntax table
   d) packet outline

16) A(n) _____ intercepts internal user requests and then processes that request on behalf of the user.
   a) content filter
   b) intrusion prevention device
   c) host detection server
   d) proxy server

17) A reverse proxy _____
   a) is the same as a proxy server
   b) routes incoming requests to the correct server
   c) must be used together with a firewall
   d) only handles outgoing requests

18) A honeypot is used for each of the following except _____.
   a) Deflect attention away from real servers
   b) Filter packets before they reach the network
   c) Provide early warning of new attacks
   d) Examine attacker techniques

19) A(n) _____ watches for attacks but only takes limited action when one occurs.
   a) network intrusion detection system (NIDS)
   b) network intrusion prevention system (NIPS)
   c) proxy intrusion device
   d) firewall

20) _____ can be used to hide information about the internal network.
   a) DHCP, firewall, and subnetting

1

b) NAT, proxy server, and subnetting
c) Firewall, DHCP, and protocol analyzer
d) NAT, proxy server, and protocol analyzer

21) If a device is determined to have an out-of-date virus signature file then Network Access Control (NAC) can redirect that device to a network by _____
a) DHCP man-in-the-middle
b) ARP poisoning
c) TCP/IP hijacking
d) a Trojan horse

22) A firewall using _____ is the most secure type of firewall.
a) stateful packet filtering
b) network intrusion detection system replay
c) reverse proxy analysis
d) stateless packet filtering

23) A(n) _____ is a set of permissions that is attached to an object.
a) Subject Access Entity
b) security entry designator
c) object modifier
c) access control list

24) _____ is a Microsoft Windows feature that provides centralized management and configuration of computers and remote users who are using Active Directory.
a) Group Policy
b) AD Management Services
c) Resource Allocation Entities
d) Windows Register Settings

25) The principle known as _____ in access control means that each user should only be given the minimal amount of privileges necessary for that person to perform their job function.
a) Mandatory Limitations
b) Enterprise Security
c) deny all
d) least privilege

II. Jawablah secara singkat dan jelas.

1. **{15%} Pilih hanya satu (1)** dari soal berikut ini, sertakan **gambar/ bagan alur** untuk memperjelas jawaban anda.
   a. Jelaskan mekanisme yang dilakukan aplikasi sniffer semacam cain & abel untuk memperoleh password dari berbagai jenis aplikasi berbasis jaringan
   b. Jelaskan mekanisme melakukan MITM Attack pada perangkat switch.
   c. Bagaimana suatu DHCP server dapat dilumpuhkan/ dipalsukan?
   d. Jelaskan mekanisme TCP *session hijacking*.
   e. Jelaskan pengertian Vulnerability Scan, kemudian beri contoh implementasinya

2. **{20%}** Standar otentikasi yang **didukung oleh 802.11** adalah *Open System Authentication* dan *Shared Key Authentication*. **Jelaskan** kedua metode tersebut beserta gambar ilustrasinya.

3. **{10%}** WEP memiliki celah keamanan, jika dimiliki data-data sebagai berikut:

Paket 1	: IV 12345	Ciphertext 1	01110101
Paket 222	: IV 12345-	Ciphertext 222	10001011
Paket 333	: IV 12345-	Ciphertext 333	11001010

   Dan telah diketahui bahwa Plaintext 1 : 11010011
   Tunjukkan penghitungan beserta hasilnya untuk menukan nilai **Plaintext 222!**

4. **{10%}** Lengkapi mekanisme keamanan yang sesuai pada tabel berikut:

Security Model	Category	Security Mechanism
WPA Personal	Authentication	(a) .....
WPA Personal	Encryption	(b) .....
WPA2 Personal	Authentication	(c) .....
WPA2 Personal	Encryption	(d) .....
WPA Enterprise	Authentication	(e) .....
WPA Enterprise	Encryption	(f)
WPA2 Enterprise	Authentication	(g) .....
WPA2 Enterprise	Encryption	(h) .....

5. **{20%}** Uraikan langkah-langkah yang harus dilakukan oleh Administrator Jaringan Perusahaan ABC untuk melakukan konfigurasi pada server windows dengan tujuan:
   Mengelola hak akses seorang **pegawai baru** bernama **Bisma** yang diterima di divisi **Pemasaran**. Sebagai pegawai baru bisma hanya boleh **membaca** berkas-berkas dalam *share folder* yang dimiliki oleh perusahaan dengan nama **Data_Pemasaran**.
   Gunakan diagram alir (*flow chart*) atau diagram aktivitas (*activity diagram*) untuk menggambarkan langkah-langkah yang diperlukan secara lengkap

– SELAMAT MENGERJAKAN –

UJIAN TENGAH SEMESTER 2014/2015

Ujian Tengah Semester Genap 2014/2015
Jurusan Ilmu Komputer/Informatika
FSM Universitas Diponegoro Semarang

Mata Kuliah	: Keamanan Jaringan	Hari/ Tanggal	: Selasa, 21 April 2015
Beban	: 3 SKS	Jam	: 08.00 – 09.30 WIB
Dosen	: -Sutikno, ST, M.Cs	Waktu	: 90 Menit
	-Indra Waspada, ST, MTI	Sifat	: Buku tertutup

Perhatian: Segala bentuk **KECURANGAN** (mencontek teman, memberi contekan, mencontek catatan, kerja sama dan sejenisnya) akan diberikan nilai **0 (NOL)**.

Jawablah Pertanyaan dibawah ini dengan singkat dan jelas ?

1. Keadaan yang bebas dari bahaya atau risiko disebut dengan …
2. Keamanan informasi dimaksudkan untuk melindungi informasi yang memiliki nilai yang berasal dari karakteristik informasi. Sebutkan 3 karakteristik informasi tersebut ?
3. Suatu peristiwa atau obyek yang dapat mengalahkan langkah-langkah keamanan di tempat dan mengakibatkan kerugian disebut dengan …
4. Seseorang atau hal yang memiliki kekuatan untuk melaksanakan ancaman disebut dengan …
5. Kelemahan yang memungkinkan agen untuk memotong ancaman keamanan disebut dengan …
6. Seseorang yang menggunakan keterampilan komputer canggih untuk menyerang komputer hanya untuk mengekspos kelemahan keamanan disebut dengan …
7. Seseorang yang ingin masuk kedalam sistem komputer untuk membuat kerusakan kemudian Men-download software *hacking* otomatis dari situs web dan menggunakannya untuk masuk kedalam sistem komputer di sebut dengan…
8. Sebutkan 5 langkah yang membentuk serangan?
9. Sebutkan 5 prinsip dasar keamanan dalam mempertahankan terhadap serangan?
10. Jenis virus komputer yang berpura-pura menggantikan file yang akan di akses disebut dengan…
11. Jelaskan dengan singkat perbedaan utama worm dengan virus?
12. Perangkat lunak yang mencurigakan (*malicious*) yang dapat merusak sebuah sistem atau jaringan, di mana seolah-olah program tersebut merupakan program baik-baik disebut dengan …
13. Suatu *malware* yang mengganti perintah sistem operasi dengan versi modifikasi disebut dengan …
14. Email yang tidak diharapkan di sebut dengan istilah ….
15. Sebutkan 2 karakteristik *spyware* yang membuat sangat berbahaya?
16. Sebuah perangkat komputer atau program yang memonitor tombol komputer yang sedang di ketik oleh user disebut dengan …
17. Sebuah komputer yang terinfeksi dengan sebuah program yang akan memungkinkan penyerang untuk kontrol jarak jauh disebut dengan …
18. Jelaskan alasan singkat mengapa BIOS (*Basic Input Output System*) dapat di gunakan sebagai objek serangan?
19. Sebutkan 3 pendekatan dalam perlindungan sistem operasi untuk melawan serangan?

20. Sebutkan 2 pertahanan serangan dengana *buffer overflow* pada sistem berbasis windows?
21. Jenis aksi *hacking* pada keamanan komputer di mana seorang penyerang bisa mendapatkan akses ke basis data di dalam sistem disebut dengan ...
22. Proses dari sumber daya atau layanan yang diberikan atau di tolak oleh sistem komputer atau jaringan disebut ...
23. Model kontrol akses yang tidak membatasi dan Subjek memiliki total kontrol atas objek yang dia memiliki disebut dengan ...
24. Serangan terhadap password yang mencoba untuk menebak password melalui penggabungkan kombinasi karakter acak disebut ...
25. Sebuah perangkat keamanan yang memantau dan mengontrol dua pintu ke sebuah ruangan kecil (ruang depan) yang memisahkan area tidak aman dari daerah aman disebut dengan ...
26. Protocol yang dirancang untuk menyediakan *strong authentication* untuk aplikasi client/server menggunakan kombinasi *secret key* dan *public key cryptography* disebut dengan ...
27. Proses mengubah teks asli pesan rahasia menggunakan kriptografi disebut dengan ...
28. Sebutkan 3 informasi yang terdapat pada Sertifikat digital?
29. Sebutkan 4 Komponen dalam PKI (*Public Key Infrastructure*) ?
30. Apa hasil dari algoritma *transposition ciper* dengan plaintext "ADA LIMA ORANG ASING BERADA DI GEDUNG" jika digunakan kunci dan nilai angka sebagai berikut:

S	E	M	A	R	A	N	G
8	3	5	1	7	2	6	4

~tik190415~

?