Ujian Tengah Semester (UTS) Susulan  
II3230 – Keamanan Informasi – 2024

# Pernyataan

Saya mengerjakan UTS susulan ini secara mandiri, tidak melihat jawaban dari catatan atau dari orang lain (nyontek), dan tidak menggunakan Google (search engine) atau tools sejenisnya (ChatGPT dll.). Jawaban ini saya berikan berdasarkan pemahaman saya saja. Saya juga tidak mengubah pekerjaan UTS mahasiswa lain.

<…………………………..>

# Pilihan Berganda

Tandai pilihan Anda dengan lingkaran atau silang.

1. Program yang dapat digunakan untuk mendeteksi penerobosan (intrusion)
2. Etherpeek b. Wireshark c. Snort d. Hydra
3. Memalsukan alamat IP dapat disebut
4. Spoofing b. Sniffing c. Password cracking d. Smurfing
5. TCP flag yang digunakan untuk melakukan reset adalah
6. SYN b. FIN c. RST d. URG e. RES
7. Postfix adalah contoh dari
8. Web server b. FTP server c. Proxy server d. Patch server e. Mail server
9. Mana yang **bukan** fungsi dari program nmap

a. Memetakan (mapping) jaringan b. Port scanning c. OS detection

d. Melakukan ping

1. Di dalam dunia keamanan informasi (information security) dikenal dengan istilah “CIA”. Apa kepanjangan dari CIA?
2. Confidentiality, Integrity, Authentication
3. Conformance, Integrity, Authentication
4. Confidentiality, Integrity, Auditability
5. Confidentiality, Integrity, Availability
6. Dalam hal otentikasi (*authentication*), mana yang tidak benar
7. Sesuatu yang dimiliki b. Sesuatu yang diketahui

c. Sesuatu yang melekat kepada seseorang d. Sesuatu yang dikirimkan

1. Mana yang tidak dapat dibenahi (dipecahkan) dengan menggunakan kriptografi?

a. Confidentiality b. Availability c. Authentication d. Integrity

1. *Denial of Service* (DoS) merupakan serangan terhadap aspek?

a. Confidentiality b. Availability c. Authentication d. Integrity

1. Mengapa kita harus menggunakan HTTPS dibandingkan HTTP?
2. HTTPS lebih hemat bandwidth
3. HTTPS lebih aman karena menggunakan kriptografi
4. HTTPS lebih umum digunakan
5. HTTPS lebih didukung oleh web browser
6. Password mana yang lebih aman
7. 9326712498276
8. BuDiRaHaRdJo
9. Qp92!!ha
10. JKTINDO123
11. Salah satu solusi terhadap masalah **ransomware** adalah:
12. Menggunakan protokol HTTPS
13. Menggunakan protokol SSH
14. Backup & Restore
15. Menggunakan public & private key (PKI)
16. Cara untuk mendeteksi adanya serangan (*attack*) adalah
17. Menganalisis log
18. Menggunakan IDS
19. Menerapkan SIEM (*Security Incident and Event Management*)
20. Semuanya benar
21. Mengapa melakukan investigasi terhadap sistem elektronik/digital tidak mudah?
22. Adanya data yang terenkripsi
23. Pelaksanaan investigasi harus dalam koridor hukum yang berlaku (privasi, chain of custody)
24. Tidak ada tools yang memadai
25. Semuanya benar

# Isian

Jawablah pertanyaan berikut ini dengan jawaban yang singkat.

1. Sebutkan minimal dua (2) perbedaan dari algoritme kriptografi kunci privat dan kunci publik.

Jawaban:

1. Sebutkan port-port yang biasanya digunakan oleh masing-masing layanan berikut ini:
2. HTTPS: b. FTP: c: SCP: d: SMTP:

# Mencocokkan

Cocokkan kata-kata di kolom sebelah kiri dengan kata-kata yang berada di kolom sebelah kanan. Letakkan huruf jawaban di kolom kanan pada kolom kiri.

|  |  |
| --- | --- |
| 1. Snort (…) | 1. Social engineering |
| 1. HTTPS (…) | 1. Kartu ATM |
| 1. DNS (…) | 1. Password cracker |
| 1. Hydra (…) | 1. IDS |
| 5. Wireshark (…) | e. Mail |
| 6. Shouldering (…) | f. .ID |
| 7. Skimming (…) | g. Sniffer |
| 8. Spam (…) | h. SSL |