Ujian Tengah Semester
Semester Genap Tahun **Ajaran 2016/2017**
Program Studi Teknik Informatika
Departemen Teknik Informatika & Komputer
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
Kampus PENS J. Raya ITS Keputih Sukolilo, Surabaya 60111

FM-VVS.01.Rev.00

Mata Kuliah	**: Keamanan Data**	**Dosen**	**: Ferry Astika Saputra**
Kelas	**: 2 D4LJ IT**	**Sifat**	**: Terbuka**
Waktu	**: 70 menit/15:30-16:40**	**Hari / Tgl.**	**: Senin, 3 April 2023**

1. "Dalam perspektif DFIR, data terbagai menjadi 2 jenis, yaitu *data at rest* dan *data in transit*. Dan secara konsep, keamanan informasi menerapkan prinsip CIA."
   Jelaskan pernyataan tersebut (apabila memungkinkan sertai dengan gambar)! (bobot 30%)
2. Jelaskan apa yang dimaksud dengan cyber security! Berikan juga contoh kasus dan impactnya! (bobot 20%)
3. Jelaskan hubungan antara *threat, vulnerability, risk* dan *impact*! Jelaskan dahulu definisinya! (bobot 30%)
4. Which of the following controls can be used to protect data that is traversing the network? (2%)
   - Firewall
   - Intrusion Detection System
   - Virtual Private Network (VPN)
   - Anti Virus Software
5. Which of the following activities is related to vulnerability management (2%)
   - Updating antivirus software signature
   - Enforcing VPN usage on corporate users
   - Applying new firewall rules
   - Applying security patches
6. Securing the data centre with locks and closed-circuit television (CCTV) is an example of which security control category? (2%)
   - Policy
   - Physical
   - Virtual
   - Technical
7. Cyber Security Frameworks can help organizations to (2%)
   - Protect critical services and information assets
   - Develop policies and procedures for the implementation of security controls

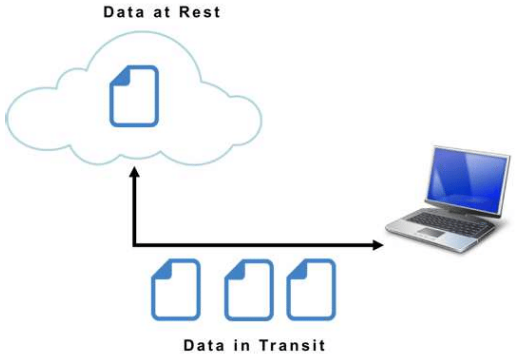
- Detect intrusion attempts and log them to a central repository
- Secure the network perimeter from unauthorized access

8. Which of the following security controls can be used to limit access to certain servers hosted in a facility? (2%)
   - Packet Analysis Tool
   - Firewall
   - Network Monitoring System
   - Intrusion Detection System
9. Access to an internal server can be limited by using which of the following security control? (2%)
   - Patch Management
   - Firewall
   - Network Monitoring
   - Intrusion Detection System
10. Reviewing access and activities from log files is an example of which of the following security controls? (2%)
    - Vulnerability management
    - Incident Response
    - Authentication
    - Security Audit
11. One of the responsibilities of a security auditor is to(2%)
    - Ensure compliance to security policies
    - Analyze logs and netflows for signs of attacks
    - Configure firewall rules
    - Write signatures for the intrusion detection system
12. Which role is responsible for ensuring internally developed web applications are not vulnerable to attacks such as SQL injection or Cross-Site Scripting? (2%)
    - Software Developer
    - Security Auditor
    - Security Analyst
    - Network Engineer
13. Which role normally deals with data recovery and examination after a security breach? (2%)
    - Penetration Tester
    - Digital Forensics Analyst
    - Network Engineers
    - Security Auditor

Nama : Nadya Indah Trisnawati
Kelas : D4 LJ IT B
NRP : 3122640034

Jawaban :

1. Data dan informasi dapat berada dalam kondisi diam, digunakan, atau bergerak.
   a. Data at Rest (data diam) adalah data yang tidak aktif yang disimpan secara fisik didalam database, gudang data, lembar kerja, arsip, cadangan luar situs, dll.
   b. Data in Transit (data bergerak) adalah data yang sedang berpindah melalui jaringan atau sementara berada di memori komputer untuk dibaca atau diperbarui.



   Keamanan informasi menerapkan prinsip CIA memiliki beberapa contoh yaitu :
   a. Kerahasiaan (Confidentialy) adalah sifat informasi yang tidak dibuat tersedia atau diungkapkan kepada individu, entitas, atau proses yang tidak berwenang.
      Contoh : nama pengguna dan kata sandi (atau kredensial pengguna) untuk mengakses webmail harus diketahui hanya oleh pengguna. Konten komunikasi email harus hanya tersedia untuk penerima yang dimaksud.
   b. Integritas (Integrity) adalah sifat menjaga akurasi dan juga kelengkapan asset.
      Contoh : Email yang diterima atau dikirim tidak dimodifikasi dari bentuk aslinya.
   c. Ketersediaan (Availability) adalah Sifat yang dapat diakses dan dapat digunakan sesuai permintaan oleh entitas yang diizinkan tanpa penundaan
      Contoh : komunikasi email sangat penting bagi perusahaan, layanan email harus tersedia sepanjang waktu.

2. Cyber security adalah aktivitas yang dilakukan sistem atau seseorang dalam rangka melindungi sistem komputer dari serangan. Biasanya serangan tersebut bersifat ilegal. Cyber security melibatkan penggunaan teknologi, kebijakan, dan praktik terbaik untuk mengurangi risiko serangan siber dan melindungi informasi penting dari kebocoran atau kehilangan.
   Contoh kasus : serangan WannaCry pada tahun 2017 yang menyebar di seluruh dunia dan mempengaruhi ratusan ribu komputer, termasuk sistem kesehatan dan perusahaan. Serangan ini memanfaatkan kelemahan dalam sistem operasi Windows dan meminta pembayaran dalam bentuk Bitcoin untuk memulihkan akses ke data yang terenkripsi. Dampak dari serangan siber seperti WannaCry bisa sangat merusak, terutama jika data penting menjadi tidak tersedia atau diambil oleh pihak yang tidak sah. Serangan serupa juga dapat menyebabkan kerugian finansial dan reputasi bagi organisasi yang terkena dampaknya. Oleh karena itu, cyber security menjadi semakin penting dalam menghadapi ancaman siber yang semakin kompleks dan sering terjadi.

3. Definisi dan hubungan *threat*, *vulnerability*, *risk* dan *impact* yang merupakan konsep-konsep penting dalam dunia keamanan siber. Mereka saling terkait dan penting untuk dipahami dalam rangka menjaga keamanan sistem komputer dan jaringan.
    a. Threat (Ancaman), penyebab potensial dampak yang tidak di inginkan terhadap sistem atau organisasi. Ancaman ini dapat berupa serangan siber, virus, malware, atau upaya peretasan. Ada beberapa kategori ancaman yaitu ancaman alam yang mengacu pada banjir, gempa bumi dll, ancaman manusia yaitu peristiwa yang diaktifkan disebabkan oleh manusia seperti pengetikan tidak sengaja atau tindakan yang disengaja, ancaman lingkungan yang mengacu pada kegagalan daya listrik jangka panjang, polusi, bahan kimia dll.
    b. Vulnerability (Kerentanan), kelemahan dalam prosedur keamanan sistem, desain, implementasi, atau control internal yang dapat dieksploitasi (dipicu secara tidak sengaja atau dimanfaatkan secara sengaja) dan mengakibatkan pelanggaran keamanan atau pelanggaran kebijakan keamanan sistem. Kerentanan ini dapat terjadi karena kekurangan dalam perangkat lunak, konfigurasi yang buruk, atau kebijakan keamanan yang lemah.
    c. Risk (Resiko), kemungkinan sumber ancaman tertentu mengeksploitasi kerentanan potensial dan dampak yang dihasilkan dari kejadian buruk tersebut pada organisasi. Risiko ini dapat dihitung dengan mempertimbangkan ancaman, kerentanan, dan dampak dari serangan.
    d. Impact, Tindakan ini memeriksa pengaruh (impact) dari serangan atau ancaman yang terjadi dalam sebuah jaringan. Dampak ini dapat mempengaruhi keberlangsungan bisnis dan kepercayaan pelanggan.

    Dalam upaya untuk melindungi sistem dan jaringan, perlu dilakukan pengukuran dan manajemen terhadap threat, vulnerability, risk, dan impact. Dengan memahami konsep-konsep tersebut, organisasi dapat meningkatkan keamanan sistem dan jaringan mereka dengan cara yang lebih efektif dan terstruktur

4. C. Virtual Private Network (VPN)
5. D. Applying Security Patches
6. B. Physical
7. B. Develop Policies and Procedures for the implementation of security control
8. B. Firewall
9. B. Firewall
10. D. Security Audit
11. A. Ensure Compliance to to Security Policies
12. A. Software Developer
13. B. Digital Forensic Analyst