LAPORAN

KEMANAN JARINGAN

Teacher : Dr. Ferry Astika Saputra ST, M.Sc

UTS

DISUSUN OLEH :

SYIHAB MUHAMMAD UBAIDILLAH

3122640043

PROGRAM STUDI TEKNIK INFORMATIKA

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

D4 TI LANJUT JENJANG

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

JAWABAN

1. CIA adalah model stander dalam keamanan informasi yang dirancang untuk mengatur dan mengevaluasi bagaimana sebuah organisasi atau perusahaan ketika data disimpan, dikirim atau diproses. Setiap aspek yang ada didalam CIA triad (Confidentiality, Integrity, Availability) akan menjadi komponen penting dari keamanan informasi. Berikut penjelasan singkat mengenai CIA :

   Confidentiality (Kerahasiaan), ketika membahas kerahasiaan informasi tentunya kita sedang berbicara mengenai serangkaian upaya perlindungan agar informasi atau data tidak terakses oleh pihak yang tidak berwenang.

   Integrity , dalam keamanan informasi integritas mengacu oada suatu metode untuk menjada agar data atau informasi tidak dapat dimanipulasi, diubah atau diedit oleh pihak yang tidak mempunyai wewenang.

   Availability, dalam konteks kemanan informasi upaya menjaga agar sebuah sistem tetap bisa digunakan adalah hal yang penting dilakukan. Dengan memberikan perlindungan availability , kita harus bisa memberikan jaminan bahwa sistem dan data dapat diakses oleh pengguna yang diautentikasi kapanpun informasi tersebut dibutuhkan.

   Selanjutnya mengenai perspektif DFIR yang membagi data menjadi dua macam, yakni *data at rest* dan *data in transit.*

   Data at rest ialah data yang tidak aktif disimpan secara fisik didalam database, gudang data, lembar kerja, arsip, dan lain sebagainya.

   Data in transit ialah data yang sedang berpindah melalui jaringan atau sementara berada di memori komputer untuk dibaca atau diperbarui.

   Dikarenakan hal tersebut membahas antara CIA dan persprektif DFIR, dimana hal ini sama-sama untuk menjaga keamanan informasi agar tidak dapat diakses oleh pihak yang tidak berwenang, baik dalam bentuk data yang sudah tidak aktif ataupun masih aktif, dikarenakan ini adalah sebuah data yang memang seharusnya dijaga dari pihak yang tidak berwenang. Penerapan CIA pada kedua data tersebut (*data at rest* dan *data in transit*) merupakan sebuah keharusan yang harus dilakukan oleh sebuah perusahaan/instansi.

2. Cybersecurity adalah proses perlindungan sistem, data, jaringan dan program dari ancaman atau serangan digital.

   Contoh kasus penerapan cybersecurity saya berikan dari pengalaman pribadi saya waktu masih di pondok pesantren, tepatnya pada tahun 2021 sebelum pembukaan penerimaan santri baru, pesantren ingin memperbaharui hardware seluruh komputer pesantren, singkat cerita semua komputer sudah diperbaharui baik dari software begitu juga hardware. Namanya juga komputer pesantren pastinya akan menginstal banyak aplikasi dan mempunyai ribuan data yang ada, pada awalnya tidak ada apa-apa pada komputer tersebut, namun dikarenakan lalai ataupun ketidaktahuan petugas mengenai cybersecurity, komputer yang tadinya normal dapat dipakai sebagaimana mestinya mendadak langsung mati, waktu di hidupkan kembali pada *data explorer* semua file berubah format menjadi ".gujd", baik dokumen, foto, video dsb formatnya berubah

menjadi “photo.img.gujd“. Dicari tahu lebih lanjut ternyata ini adalah bentuk serangan ransomware yang dilakukan oleh pihak yang tidak bertanggung jawab, ransomware ini merupakan sebuah malware yang bisa mengenkripsi semua file di sistem pengguna. Setelah file tersebut berubah kemudian pelaku akan menuntut uang tebusan agar semua file didekripsi. Hal ini dikarenakan kurangnya pengetahuan dengan adanya serangan seperti halnya ransomware, phising dan DdoS.

3. *Threat* adalah penyebab potensial dari dampak yang tidak diinginkan terhadap sistem atau organisasi.
   Vulnerability adalah kelemahan dalam prosedur keamanan sistem, desain, implementasi atau kontrol internal yang dapat dieksploitasi dan mengakibatkan pelanggaran keamanan atau pelanggaran kebijakan keamanan sistem.
   Risk adalah kemungkinan sumber ancaman tertentu mengkploitasi kerentanan potensial dan dampak yang dihasilkan dari kejadian buruk tersebut pada organisasi.
   Impact adalah efek ancaman atau penyerangan yang terjadi dalam sebuah jaringan.
   Hubungan antara keempat hal tersebut ialah sebuah bentuk kelemahan atau kerugian yang ditimbulkan dikarenakan kurangnya dalam penjagaan atau perawatan keamanan jaringan. Penting bagi kita dalam menjaga sebuah informasi agar tidak disalah gunakan apalagi dapat diambil oleh pihak yang tidak bertanggung jawab.