Nama : Saint Ripen Tumanggor (22111942)
Kelas : IF – C Pagi

Tugas 1: Keamanan Informasi
TASK I (A)

1. Adware (Advanced Persistent Threat - APT)
    - Deskripsi: Adware adalah perangkat lunak yang dirancang untuk menampilkan iklan pada perangkat pengguna. Meskipun tujuannya seringkali komersial, adware yang lebih canggih bisa digunakan untuk memperoleh akses tak sah ke data pengguna.
    - Ancaman: APT adalah serangan berkelanjutan yang bertujuan untuk mencuri informasi secara diam-diam tanpa terdeteksi.

2. Backdoors
    - Deskripsi: Backdoor adalah jalur tersembunyi yang memungkinkan pengguna (atau penyerang) untuk mengakses sistem tanpa otentikasi yang normal.
    - Ancaman: Penyerang dapat mengambil alih perangkat atau sistem jika backdoor digunakan untuk melewati kontrol keamanan.

3. Cryptojacking Malware
    - Deskripsi: Malware ini digunakan untuk memanfaatkan daya komputasi perangkat korban guna menambang mata uang kripto tanpa izin pengguna.
    - Ancaman: Selain merusak perangkat, cryptojacking dapat menguras sumber daya yang dapat menyebabkan penurunan kinerja sistem.

4. SQL Injection
    - Deskripsi: SQL injection terjadi ketika penyerang menyisipkan kode SQL berbahaya ke dalam formulir input untuk memanipulasi basis data.
    - Ancaman: Dapat mengakses, mengubah, atau menghapus data yang ada dalam database.

5. Phishing
    - Deskripsi: Phishing adalah teknik penipuan yang menggunakan email atau situs web palsu untuk memperoleh informasi pribadi seperti kata sandi dan nomor kartu kredit.
    - Ancaman: Data pribadi dapat dicuri dan digunakan untuk melakukan kejahatan identitas.

6. Ransomware
    - Deskripsi: Ransomware adalah jenis malware yang mengenkripsi file di sistem korban dan meminta tebusan untuk mengembalikannya.
    - Ancaman: Dapat menyebabkan kerugian finansial dan gangguan operasional bagi korban.

7. Malware
    - Deskripsi: Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak, mengakses, atau mencuri informasi dari sistem komputer.
    - Ancaman: Bisa melibatkan berbagai bentuk, seperti virus, trojan, dan worms, yang dapat menghancurkan data atau mengambil kendali perangkat.

8. Denial of Service (DoS)
    - Deskripsi: Serangan DoS bertujuan untuk membuat layanan atau aplikasi tidak dapat diakses dengan membanjiri sistem atau jaringan dengan permintaan palsu.
    - Ancaman: Dapat menyebabkan gangguan serius pada layanan yang bergantung pada jaringan, seperti website atau server.

9. Privilege Escalation
    - Deskripsi: Terjadi ketika penyerang memperoleh akses yang lebih tinggi dalam sistem atau aplikasi dari akses terbatas.
    - Ancaman: Memberi penyerang kontrol penuh atas perangkat atau sistem yang lebih besar, berpotensi mencuri data sensitif.

10. Spyware
    - Deskripsi: Spyware adalah perangkat lunak yang mengumpulkan data dari perangkat pengguna tanpa izin.
    - Ancaman: Dapat mencuri informasi pribadi dan mengirimkannya ke pihak ketiga yang berbahaya.

TASK I (B)

1. Secure Coding
    - Deskripsi: Praktik menulis kode perangkat lunak dengan mempertimbangkan keamanan dari awal pengembangan.
    - Tujuan: Mencegah kerentanannya yang bisa dimanfaatkan oleh penyerang, seperti injeksi kode atau buffer overflow.

2. Firewall
    - Deskripsi: Firewall adalah sistem yang memantau dan mengontrol lalu lintas jaringan yang masuk atau keluar berdasarkan aturan keamanan.
    - Tujuan: Melindungi sistem dari akses tak sah dengan membatasi lalu lintas yang tidak sah.

3. Multi-factor Authentication (MFA)
    - Deskripsi: MFA adalah metode autentikasi yang memerlukan lebih dari satu bukti identitas dari pengguna, misalnya kombinasi kata sandi dan kode OTP (One-Time Password).
    - Tujuan: Mengurangi kemungkinan akses tak sah bahkan jika kata sandi bocor.

4. Encryption
    - Deskripsi: Teknik untuk mengubah data menjadi format yang tidak dapat dibaca tanpa kunci tertentu.
    - Tujuan: Melindungi data sensitif agar tidak dapat diakses meski dicuri.

5. Antivirus Software
    - Deskripsi: Program perangkat lunak yang dirancang untuk mendeteksi dan menghapus virus serta ancaman lainnya dari komputer.
    - Tujuan: Mencegah malware mengakses atau merusak perangkat.

6. Intrusion Detection System (IDS)
    - Deskripsi: Sistem yang memantau lalu lintas jaringan untuk mendeteksi potensi ancaman atau serangan.
    - Tujuan: Memberikan peringatan dini tentang potensi serangan yang terjadi dalam jaringan atau sistem.

7. Security Information and Event Management (SIEM)
    - Deskripsi: Sistem yang mengumpulkan dan menganalisis data keamanan dari berbagai sumber untuk mendeteksi dan merespons ancaman.
    - Tujuan: Membantu organisasi dalam mengelola dan merespons insiden keamanan secara lebih efisien.

TASK II

1. Data Protection Policy (Kebijakan Perlindungan Data)
   - Deskripsi: Kebijakan ini mengatur bagaimana data pribadi dan sensitif dilindungi di organisasi.
   - Referensi:
     General Data Protection Regulation (GDPR): Regulasi dari Uni Eropa yang mengatur perlindungan data pribadi.
     - Link: https://gdpr.eu/

2. Logging and Monitoring Policy
   - Deskripsi: Kebijakan ini mengatur pencatatan aktivitas sistem, pemantauan real-time, dan perlindungan log untuk mendukung audit dan deteksi ancaman, sesuai dengan standar keamanan seperti NIST.
   - Referensi: NIST Special Publication 800-92 (Guide to Computer Security Log Management)
     - Link: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf (diterbitkan September 2006, tetap menjadi referensi utama hingga Maret 2025).

3. Access Control Policy
   - Deskripsi: Kebijakan ini menerapkan kontrol akses berbasis peran, autentikasi multi-faktor (MFA), dan prosedur pencabutan akses untuk memastikan hanya pengguna yang berwenang yang dapat mengakses sistem.
   - Referensi: ISO/IEC 27001:2013 (Information Security Management)
     - Link: https://www.iso.org/standard/54534.html (diperbarui 2013, tetap berlaku hingga Maret 2025, akses mungkin memerlukan pembelian dokumen).

4. Training and Awareness Documents
   - Deskripsi: Kebijakan ini mensyaratkan pelatihan rutin tentang kesadaran keamanan siber, termasuk pengenalan phishing dan tanggung jawab karyawan, dengan jadwal dan evaluasi kepatuhan.
   - Referensi: SANS Institute - Security Awareness Training Guidelines
     - Link: https://www.sans.org/security-awareness-training/ (diperbarui berkala, terakhir diakses Maret 2025).

5. Cryptographic Policy
    - Deskripsi: Kebijakan ini mengatur penggunaan enkripsi untuk data sensitif, termasuk pemilihan algoritma (misalnya AES), pengelolaan kunci, dan pembaruan rutin untuk keamanan.
    - Referensi: NIST Special Publication 800-57 Part 1 Rev. 5 (Recommendation for Key Management)
        - Link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf (diperbarui Mei 2020, tetap relevan hingga Maret 2025).

6. Network Security Policy
    - Deskripsi: Kebijakan ini mengatur perlindungan jaringan dari ancaman eksternal dan internal, termasuk konfigurasi firewall, segmentasi jaringan, pemantauan lalu lintas, dan respons terhadap serangan seperti DDoS. Kebijakan ini juga mencakup penggunaan protokol aman (misalnya, HTTPS, VPN).
    - Referensi: NIST Special Publication 800-53 Rev. 5 (Security and Privacy Controls for Information Systems and Organizations)
        - Link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (diperbarui Oktober 2020, tetap relevan hingga Maret 2025).

7. Incident Response Policy
    - Deskripsi: Kebijakan ini menguraikan langkah-langkah untuk mendeteksi, merespons, dan memulihkan sistem dari insiden keamanan (misalnya, pelanggaran data), termasuk pembentukan tim respons, komunikasi dengan pihak berwenang, dan pelaporan pasca-insiden.
    - Referensi: NIST Special Publication 800-61 Rev. 2 (Computer Security Incident Handling Guide)
        - Link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (diperbarui Agustus 2012, tetap relevan hingga Maret 2025).