1. **Keamanan Siber**
   Ruang siber adalah jaringan internet yang rentan terhadap ancaman seperti hacker, malware, dan ransomware. Serangan siber dapat merusak sistem atau mencuri data, yang memerlukan pengaturan hukum siber untuk melindungi aktivitas online.
2. **IT Forensic**
   Berfungsi mengidentifikasi bukti digital dengan elemen seperti pengumpulan data, analisis, dan pelaporan untuk melacak pelaku kejahatan digital.
3. **Keamanan Pribadi**
   Pentingnya kesadaran pengguna terhadap keamanan data, kebijakan perlindungan privasi, dan hukuman bagi pelanggar keamanan siber.
4. **Manajemen Risiko**
   Mitigasi risiko dilakukan melalui rencana pemulihan bencana (Disaster Recovery Plan) dan kelangsungan bisnis (Business Continuity Plan) untuk menjaga operasional meski ada gangguan.
5. **Pentest dan Tahapannya**
   Meliputi:
   - **Reconnaissance**: Pengumpulan informasi target.
   - **Scanning**: Memeriksa kerentanan sistem.
   - **Gaining Access**: Mengeksploitasi celah untuk kontrol.
   - **Maintaining Access**: Menjaga akses yang diperoleh.
   - **Covering Tracks**: Menghapus jejak serangan.
6. **Konsep CIA**
   - **Confidentiality:** Menjaga kerahasiaan data.
   - **Integrity:** Memastikan data tidak dimodifikasi.
   - **Availability:** Sistem selalu tersedia.
7. **Kasus dan Solusi Keamanan**
   - Ransomware WannaCry: Pentingnya pembaruan sistem dan backup data.
   - Serangan DDoS GitHub: Menggunakan mitigasi seperti firewall dan bandwidth besar.
   - Phishing: Meningkatkan kesadaran pengguna dan mengimplementasikan 2FA.
   - Kebocoran Data E-Commerce: Solusi berupa firewall aplikasi, validasi input, dan kontrol akses ketat.