Tinjauan Mata Kuliah

Pada mata kuliah ini pada awalnya akan diajarkan tentang pengertian keamanan, pengertian sistem dan pengertian keamanan sistem, evaluasi keamanan sistem, mengamankan sistem informasi, keamanan *email*, keamanan *web*, eksploitasi keamanan sistem, *cyber law*, keamanan sistem *wireless*, manajemen keamanan informasi serta metode peretasan dan teknik pengamanannya.

Mata kuliah ini bertujuan untuk memberikan pengetahuan dan pengalaman secara praktis kepada mahasiswa pengertian keamanan, pengertian sistem dan pengertian keamanan sistem, evaluasi keamanan sistem, mengamankan sistem informasi, keamanan *email*, keamanan *web*, eksploitasi keamanan sistem, *cyber law*, keamanan sistem *wireless*, manajemen keamanan informasi serta metode peretasan dan teknik pengamanannya.

Modul 1 : **Pengantar Keamanan Sistem Informasi**

Pada modul ini akan diberikan pengantar tentang pengertian dan masalah keamanan sistem informasi, sehingga mahasiswa dapat memiliki nuansa tentang mata ajaran ini secara global. Dalam modul ini akan dibahas tentang berbagai contoh permasalahan dalam sistem keamanan informasi, penanggung jawab Keamanan Sistem Informasi beserta perannya, *Zero-day-attack* sebagai masalah utama dalam keamanan SI, tindakan umum untuk penyelesaian masalah *Zero-day-attack*, jenis-jenis kerawanan sistem keamanan yang sering di jumpai, Pengertian, Tujuan dan Pengelolaan Keamanan Sistem Informasi, dan Evaluasi Risiko Keamanan Informasi.
Juga dibahas tentang panduan-panduan standar pengamanan sistem seperti: *OWASP (Open Web Application Security Project), NVD-NIST (National Vulnerability Database- Information Technology Laboratory), CVE-MITRE (MITRE Corporation's documentation defines CVE Identifiers).*

Modul 2 : **Metode Kamuflase, Perlindungan dan Legitimasi Informasi**

Pada modul ini akan dibahas tentang implementasi beberapa teknik pengamanan informasi yang sering dijumpai di masyarakat umum secara manual maupun di dunia digital. Pembahasan diawali dengan Kriptografi dan *Digital Signature* dilanjutkan dengan *Watermarking* dan Steganografi.
Pada bagian ini akan dibahas tentang definisi kriptografi dan *digital signature,* klasifikasi kriptografi, *cryptographic hash function, public key infrastructure, digital signature, digital watermarking, digital steganografi,* aplikasi steganografi.

Modul 3 : ***Malware* dan Teknik Pengamanan Sistem Informasi**

Dalam modul ini akan dibahas tentang ancaman terhadap suatu sistem informasi, pengertian tentang masalah dan ancaman, cara deteksi kerentanan dan cara melakukan pengamanan suatu sistem informasi, serta memberikan alternatif solusi untuk menyelesaikan masalah. Pembahasan diawali dengan *Malware* selanjutnya dibahas tentang Pengamanan Sistem. Pada bagian ini akan dibahas tentang malware beserta seluruh faktornya, komponen otentikasi, otorisasi, kerentanan pada sistem, faktor-faktor keamanan sistem, IPS dan IDS.

Modul 4 : **Eksploitasi Keamanan Sistem Informasi**

Pada modul ini Anda akan mempelajari tentang berbagai metode *hacking* yang lazim dilakukan oleh para peretas, ataupun digunakan oleh para *penetration tester* (penguji kehandalan sistem), serta petunjuk kunci untuk mengatasi kerentanan sistem dan perangkat yang digunakan. Beberapa topik yang akan dibahas mencakup: definisi pengumpulan informasi dan rekayasa Sosial, teknik-teknik pengumpulan informasi, rekayasa sosial yang lazim terjadi, cara penggunaan *Search Engine* untuk pengumpulan informasi, cara penggunaan media sosial untuk pengumpulan informasi serta Teknologi Website yang terkait keamanan sistem :*HTTP Protocol Basic, Cookies, Session, Proxy, SQL Injection, Cross Site Scripting (XSS).*

Modul 5 : **Teknologi Pengamanan Perangkat Jaringan Nirkabel dan *Email***

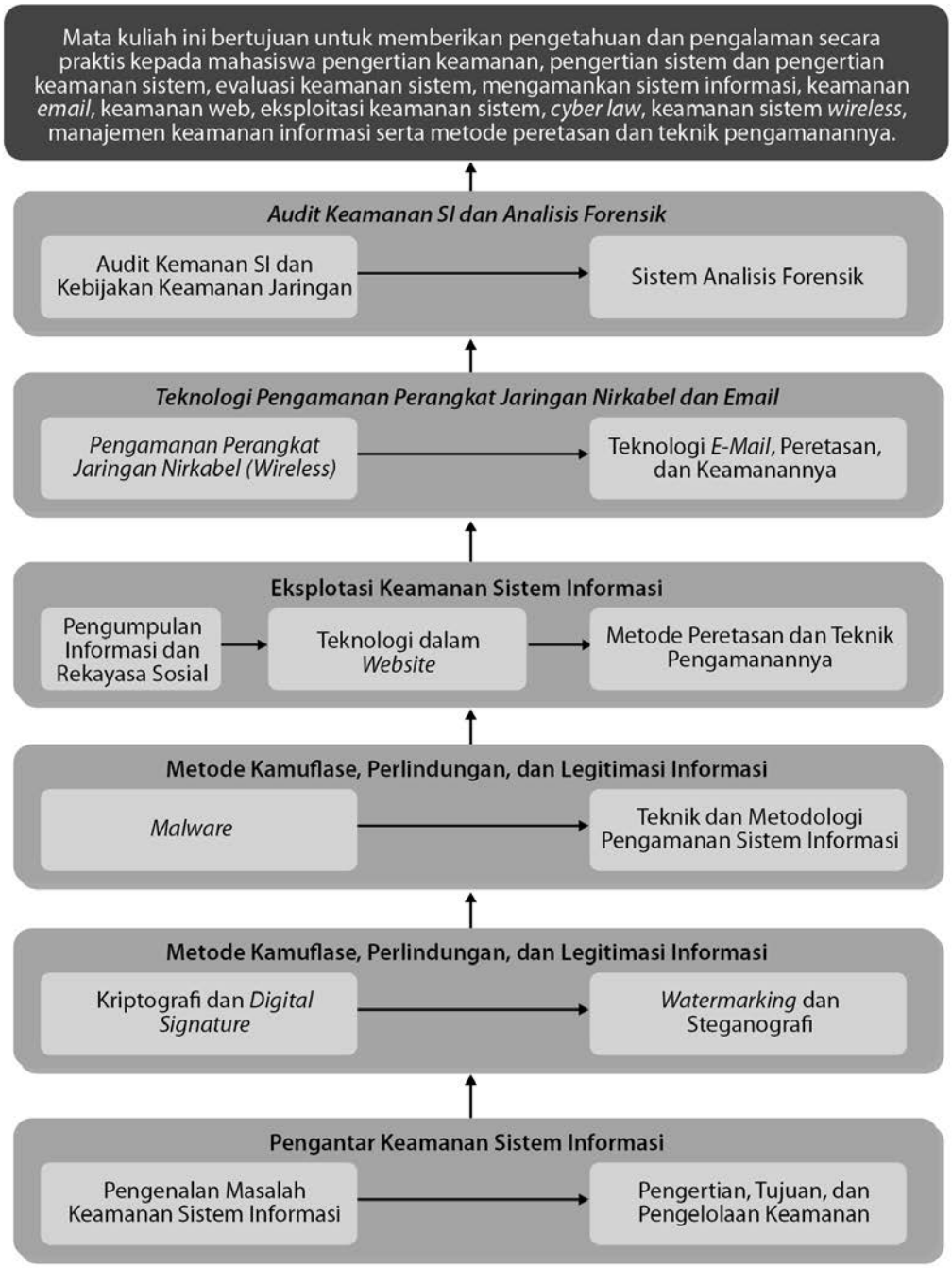
Pada modul ini akan dibahas masalah keamanan pada jaringan nirkabel (*wireless*) dan *email.* Terkait dengan hal tersebut maka akan dibahas tentang pengertian dan tujuan keamanan pada kedua sistem tersebut serta dapat mengatasi dan mengantisipasi masalah-masalah keamanan yang sering timbul pada kedua sistem tersebut.

Beberapa topik yang akan dibahas mencakup: konsep keamanan sistem nirkabel (*wireless),* teknologi dan peralatanan pada jaringan nirkabel, tipe enkripsi pada jaringan nirkabel, permasalahan pada jaringan nirkabel, ancaman pada jaringan nirkabel, metode peretasan sarana nirkabel Menjelaskan tentang pada jaringan *bluetooth,* sistem pertahanan atas serangan pada jaringan *wirelessv,* sistem pertahanan atas serangan pada jaringan *bluetooth,* tindakan kriminal dengan *email,* investigasi *email.*

Modul 6 : **Audit Keamanan SI dan Analisis Forensik**

Pada modul ini akan dibahas langkah-langkah pengamanan sistem informasi yang meliputi pembuatan kebijakan, deteksi, pemantauan, pengamanan. Selain itu juga akan dibahas *system forensics analysis* suatu sistem informasi.

Beberapa topik yang akan dibahas mencakup: Pengelolaan keamanan sistem (ISMS), cara/sistem Audit Keamanan Informasi Dan Kebijakan Keamanan Jaringan, Infrastruktur sistem Keamanan Jaringan , analisa atas data keamanan jaringan *(Network Security Data)*, Teknologi pemantauan sistem dan jaringan , protokol dalam pemantauan sistem dan jaringan, analisa dan evaluasi atas data peringatan dari sistem *(System Alert)*, Sistem Analisa Forensik dan data, Penanganan Barang Bukti Dan Penindakan, konsep *"The Cyber Kill Chain"*, konsep *"The Diamond Model Of Intrusion Analysis"*, konsep Insiden Respons, penanganan atas insiden.

.

Peta Kompetensi
MSIM4405/Keamanan Sistem Informasi/2 SKS