Tinjauan Mata Kuliah

Pada mata kuliah ini bagian awalnya diajarkan tentang pengertian, ruang lingkup dan gangguan keamanan jaringan dilanjutkan dengan dasar-dasar keamanan jaringan dan *tools* pemantauan jaringan. Pembuatan Firewall dan VPN merupakan pengulangan dan pendalaman dari mata kuliah MSIM4316 Administrasi Jaringan; dilanjutkan dengan *intrusion detection & prevention system*. Mitigasi resiko dan pembuatan kebijakan merupakan bagian dari pengamanan jaringan secara manajerial. Sedangkan kriptografi, *autentikasi* dan *signature* merupakan pendalaman secara dasar keilmuan tentang keamanan jaringan; dan implementasi deteksi, pemantauan dan pengamanan layanan merupakan bagian implementasi secara teknis. Pada bagian akhir dibahas resume dari buku materi pokok ini yakni tentang *cyber attack*, pemantauan, pencegahan dan solusi atas masalah disertai dengan praktiknya.

Modul 1 : **Keamanan dan Ancaman pada *Cyberspace***

Sebagai dasar dalam mempelajari keamanan jaringan, perlu dipelajari dan dipahami terlebih dahulu yang dimaksud dengan istilah-istilah *cyber*, diantaranya *cyberspace, cyberlaw, cyber security* dan hal-hal yang termasuk aspek-aspek keamanan informasi, manajemen risiko, keamanan informasi dan berkaitan dengan *hacker*.

Selanjutnya dalam modul ini akan dibahas tentang ancaman dan gangguan yang umum terjadi di dunia maya. Terdapat beberapa jenis dan aspek ancaman serta beberapa bentuk ancaman yang umum terjadi di dunia maya seperti *malicious software*, aktivitas *phising*, *cyberbullying*.

Modul 2 : **Metodologi dan Jenis Serangan *Cyber***

Sebagai dasar dalam mempelajari serangan *cyber*, perlu dipelajari dan dipahami terlebih dahulu metodologi yang digunakan peretas untuk menyerang sistem target. Dalam modul ini, Anda akan mengetahui tahapan-tahapan yang dilakukan peretas pada saat melakukan serangan terhadap sistem target, mulai dari tahapan mengenali target, *scanning*, mendapat akses, memelihara akses hingga menutupi jejak. Selanjutnya dalam modul ini akan dibahas pula tentang jenis-jenis serangan. Jenis-jenis serangan yang dibahas dalam modul ini, antara lain: *cracking password, sniffing, snooping, denial of service, sql injection, cross-site scripting.*

Modul 3 : **Praktikum Unit-1**

Jenis-Jenis Serangan terhadap Jaringan dan *Server*

Dalam modul ini, Anda akan melakukan beberapa praktik *scanning* menggunakan tool Look@LAN yang merupakan *scanning* berbasis pada ICMP dan *Superscan* yang merupakan *tools scanning* untuk mengetahui port yang aktif pada suatu target. Anda juga akan mensimulasikan

mekanisme DHCP dan DNS palsu yang dapat mengubah arah trafik dari pengguna. Dalam modul ini juga Anda akan mengetahui cara *hacker* melakukan aktivitas *Sniffing* secara pasif menggunakan Wireshark dan *sniffing* secara aktif memanfaatkan *tools* Cain&Abel.

Modul 4 : **Arsitektur Pengamanan Sistem dan Penerapannya**

Dalam modul ini akan dibahas pula tentang mekanisme pengamanan terhadap *host* dan perangkat jaringan. Beberapa metode pengamanan terhadap *host* dan perangkat jaringan yang dapat diterapkan antara lain AAA (*authentication, authorization, accounting*), pengamanan terhadap perangkat *switch* berupa *port security* dan pengamanan terhadap *endpoint system*. Untuk dapat lebih memahami materi, pada modul ini juga Anda akan mensimulasikan beberapa mekanisme pengamanan berupa *DHCP snooping, AAA* dan *port security*.

Modul 5 : **Sistem Pengamanan Jaringan**

Sistem pengamanan jaringan dilakukan secara berlapis. Salah satu penerapan sistem pengamanan pada arsitektur defense in depth adalah pengamanan pada lapisan perimeter. *Firewall* merupakan perangkat pengaman pada lapisan perimeter, *firewall* melindungi jaringan internal dari serangan yang berasal dari jaringan eksternal dengan melakukan mekanisme penyaringan terhadap lalu-lintas data yang melewatinya berdasarkan serangkaian aturan yang ditetapkan.

Selanjutnya dalam modul ini akan dibahas pula tentang protokol *IPsec* (*IP security*) dan VPN (*Virtual Private Network*). *IPsec* merupakan protokol untuk melindungi data yang dikirimkan melewati jaringan komunikasi data sehingga tidak dapat diintip. *Virtual Private Network* merupakan solusi pengamanan untuk melindungi data yang melewati jaringan internet

Modul 6 : ***Intrusion Detection/Prevention System***

Pada Modul 6 ini akan dibahas tentang i*ntrusion* yang merupakan aktivitas ilegal yang dapat mengganggu keamanan informasi pada suatu sistem. Bentuk *intrusion* dapat berupa kegiatan yang bersifat anomali di suatu jaringan atau *host*. Berdasarkan karakteristik dari *intrusion* tersebut kemudian dibuat *rules* dan disimpan menjadi basis data IDS/IPS. Sehingga IDS (*Intrusion Detection System*) atau IPS (*Intrusion Prevention System*) dapat mendeteksi aktivitas yang mencurigakan pada suatu sistem atau jaringan. IDS/IPS akan memonitor lalulintas data pada suatu jaringan atau mengambil data dari *file log* pada suatu *host*, kemudian IDS/IPS akan menganalisa berdasarkan data yang diperoleh dan dengan algoritma tertentu serta basis data yang dimiliki memutuskan status dan melakukan tindakan tertentu terhadap paket data tersebut.

Modul 7 : ***Kriptografi***

Pada Modul 7 ini akan dibahas tentang kriptografi atau *cryptography* yang berasal dari bahasa Yunani yaitu *kriptos* artinya "tersembunyi, rahasia"; dan *graphein*, "menulis". Kriptografi merupakan ilmu tentang menyembunyikan pesan, hingga saat ini pengertian kriptografi berkembang menjadi ilmu tentang teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa privasi dan otentikasi. Dalam modul ini akan membahas tentang kriptografi simetris maupun asimetris.

Modul 8 : **Sistem Pengamanan pada Jaringan Nirkabel & Lapisan Atas Arsitektur *TCP/IP Stack***

Dalam Modul 8 ini dibahas tentang beberapa protokol pengamanan jaringan nirkabel adalah WEP (*Wired Equivalent Privacy*), WPA (*Wifi Protected Access*) dan WPA-PSK (WPA (*Wifi Protected Accesss - Pre Shared Key*) yang akan dibahas pada modul ini; juga dibahas tentang beberapa protokol pengamanan yang digunakan pada *upper layer TCP/IP Stack*. Beberapa diantaranya adalah SSL (*Secure Socket Layer*), TLS (*Transport Layer Security*), HTTPS dan SSH (*Secure Shell*).

Modul 9 : **Sistem Manajemen Keamanan Berbasis Risiko**

Dalam modul ini akan dibahas tentang cara mengelola risiko sehingga dapat meminimalisasi dampak yang ditimbulkan jika risiko tersebut terjadi; juga tentang standar sistem manajemen keamanan informasi. Sistem yang didasarkan pada penilaian dan tingkat penerimaan risiko yang dirancang untuk menangani dan mengelola risiko secara efektif. ISO 27001 merupakan salah satu standar yang menerapkan sistem manajemen keamanan informasi

Peta Kompetensi
MSIM4404/Keamanan Jaringan/3 sks