# MODUL PERKULIAHAN:
# KEAMANAN SIBER

| Penyusun |
| --- |
| Denpasar, 1 Oktober 2024<br><br><br>(I Wayan Ardiyasa, S.Kom., M.MSI.) |

# INFORMASI MATA KULIAH

| | |
|---|---|
| **Jumlah SKS** | 4 |
| **Jenis Matakuliah** | Teori |
| **Kegiatan Pembelajaran** | Daring |
| **Persyaratan Sarana Peserta/Spesifikasi/ Tools/Media ajar yang akan digunakan** | - |

## CAPAIAN DAN DESKRIPSI MK

| Capaian Pembelajaran Mata Kuliah (CPMK) | Deskripsi Singkat MK |
|---|---|
| • CPMK-06-17: Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi.<br>• CPMK-07-4: Mampu menjelaskan dan menguasai konsep dasar teori jaringan mahasiswa mampu memahami konsep jaringan komputer, mengetahui perangkat-perangkat jaringan, protokol jaringan, OSI dan TCP/IP model, konsep IP Address dan kelas-kelas dalam IP Address, Routing dengan media virtual seperti menggunakan packet tracer, memahami jaringan nirkabel, mengetahui serangan dalam jaringan dan mengetahui firewall. | Keamanan siber adalah matakuliah yang mempelajari tentang konsep dan teknik untuk pengamanan aplikasi, sistem dan jaringan komputer serta data digital dari kejahatan cyber yang dapat menggangu proses bisnis dan mengakibatkan kerugian. |

## REFERENSI

| Referensi |
|---|
| [1] Sadikin, R. (2012). Kriptografi Untuk Keamanan Jaringan dan Implementasinya dalam bahasa java. Yogyakarta: Andi<br>[2] Weidman, G. (2014). Penetration Testing A Hands-On Introduction to Hacking.<br>[3] Situmeang, M.S (2020). Cyber Law, Bandung: Cakra 2020 |

# PENGENALAN KEAMANAN SIBER

| Capaian Pembelajaran Mata Kuliah |
| --- |
| **CPMK-06-17 Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi** |

| Indikator Penilaian |
| --- |
| 1.1 Mahasiswa mampu menjelaskan pengenalan Keamanan Siber.<br>2.1 Mahasiswa mampu menjelaskan aspek-aspek keamanan informasi.<br>3.1 Mahasiswa mampu menjelaskan jenis-jenis ancaman, serangan dan asset.<br>4.1 Mahasiswa mampu menjelaskan strategi keamanan computer.<br>5.1 Mahasiswa mampu menjelaskan Attack surfack dan Atttack tree. |

## 1. Konsep Dasar Keamanan Siber

Keamanan siber adalah upaya melindungi sistem komputer, jaringan, dan data dari serangan atau akses yang tidak sah. Pentingnya keamanan siber meningkat seiring dengan pesatnya digitalisasi di berbagai sektor, mulai dari bisnis hingga pemerintahan. Modul ini akan membahas konsep dasar, ancaman, dan praktik terbaik dalam keamanan siber.

### 1.1 Sejarah Keamanan Siber

Masalah kejahatan dengan pencurian data sudah terjadi sejak lama bahkan sebelum masa komputer modern lahir. Sebelum Perang Dunia II, sudah ada kemajuan dalam kriptanalisis Enigma. Pada tahun 1929, Biro Sandi Polandia mulai mempekerjakan ahli matematika dengan mengundang mahasiswa di Universitas Poznan untuk mengambil kelas tentang kriptologi. Pada tahun 1932, lulusan Poznan Marian Rejewski, Henryk Zygalski dan Jerzy Rozycki bekerja untuk Biro Sandi Polandia secara penuh waktu. Secara bersamaan, seorang mata-mata Prancis, Hans-Thilo Schmidt, telah menyusup ke Kantor Cipher Jerman di Berlin.

Memecahkan Enigma membutuhkan kecemerlangan teknis dan matematis, tetapi membodohi Nazi Jerman dengan berpikir bahwa mata- mata ada di pihak mereka sangat penting. Spionase Schmidt membantu Biro Sandi Polandia memperoleh dokumentasi Enigma kunci dari Jerman. Rejewski menggunakan dokumen-

dokumen itu dan memulai cryptanalysis Enigma dengan beberapa jam kerja setiap hari menjelang akhir tahun 1932.

Selama Perang Dunia II, upaya cryptanalysis militer Inggris bermarkas di Bletchley Park. Alan Turing yaitu seorang perintis ilmu komputer terkenal, dipekerjakan oleh Government Code and Cypher School Inggris pada tahun 1938 tepat sebelum Perang. Dia bekerja di bawah Dilly Knox, seorang pemecah kode senior. Sehari setelah Inggris menyatakan perang terhadap Jerman pada bulan September 1939, operasi Turing, Knox, dan GC & CS secara umum pindah ke Bletchley Park. Inggris berfokus pada memecahkan Enigma dari pangkalan itu, dan terobosan Biro Sandi Polandia dari awal 1930-an sangat penting untuk upaya tersebut. Memecahkan Enigma elektromekanik Jerman dan sandi Lorenz mungkin menjadi faktor kunci dalam kekuatan Sekutu yang memenangkan Perang pada tahun 1945. Debut ENIAC pada tahun 1946 menandai munculnya komputasi digital. Komputer mainframe PDP mendorong inovasi MIT di tahun 50-an dan 60-an. Pada awal 1970-an, banyak perusahaan besar menjadi pelanggan teknologi mainframe IBM. Data pada mainframe perusahaan sering kali merupakan rahasia dagang industri dan data sensitif yang berkaitan dengan transaksi klien. Selain itu, pemerintah AS mengidentifikasi kebutuhan untuk menjaga keamanan data yang tidak rahasia tetapi sensitif. Karya kriptografer Horst Feistel membahas kedua bidang tersebut. Cipher Lucifer-nya untuk IBM adalah pendahulu penting untuk pengembangan DES untuk National Security Agency. Jadi, keamanan informasi mendahului komputer digital, tetapi keamanan komputer dan keamanan siber lahir dari inovasi ilmu komputer yang dimulai tepat setelah Perang Dunia II. Menjaga keamanan informasi untuk sejarah data yang mendahului komputer elektronik seperti kriptografi kuno hingga hari ini berada di bawah panji keamanan informasi. Keamanan komputer dan keamanan siber adalah istilah yang sepenuhnya dapat dipertukarkan, dan memerlukan teknologi komputer digital dari ENIAC tahun 1946 hingga sekarang. Keamanan komputer dan keamanan siber adalah anak-anak dari keamanan informasi.

Keamanan TI adalah keamanan informasi yang berkaitan dengan teknologi informasi. Teknologi informasi adalah anak dari ilmu komputer. TI adalah aplikasi ilmu komputer untuk tujuan praktis, sebagian besar untuk industri mainframe, superkomputer, pusat data, server, PC, dan perangkat seluler sebagai titik akhir untuk interaksi pekerja dan konsumen PC, perangkat seluler, perangkat IoT, dan

titik akhir konsol video game untuk gaya hidup pengguna akhir. Keamanan TI mungkin dapat digunakan secara bergantian dengan keamanan siber, keamanan komputer, dan keamanan informasi jika berkaitan dengan bisnis.

## 1.2 Jenis Serangan

### A. Serangan tidak terstruktur

Salah satu serangan di mana attacker tidak memiliki pengetahuan sebelumnya tentang lingkungan tempat mereka meluncurkan serangan. Sebagian besar, dalam skenario seperti itu, mereka mengandalkan semua alat yang tersedia secara bebas. Serangan tidak terstruktur sering ditargetkan secara massal, berdasarkan kerentanan umum dan eksploitasi yang tersedia.

### B. Serangan terstruktur

Dalam kasus serangan terstruktur, tidak seperti serangan tidak terstruktur, musuh jauh lebih siap dan terencana dalam melakukan serangan. Dalam sebagian besar kasus serangan terstruktur, kami melihat bahwa penyerang menunjukkan keterampilan pemrograman tingkat lanjut mereka, dan pengetahuan tentang sistem TI dan aplikasi yang mereka targetkan. Serangan-serangan ini bisa sangat terorganisir dan sebagian besar ditargetkan ke entitas individu atau vertikal industri.

## 1.2 Apa itu Keamanan Siber

Keamanan siber mencakup perlindungan terhadap sistem, jaringan, program, dan data dari ancaman digital seperti serangan siber. Perlindungan ini melibatkan beberapa bidang, seperti keamanan jaringan, keamanan aplikasi, keamanan informasi, dan pemulihan bencana.

## 1.2 Prinsip Keamanan Siber

a. **Kerahasiaan (Confidentiality):** Menjaga informasi agar hanya diakses oleh pihak yang berwenang.

b. **Integritas (Integrity):** Memastikan data tetap akurat dan tidak diubah oleh pihak yang tidak sah.
c. **Ketersediaan (Availability):** Menjamin bahwa sistem dan data selalu tersedia bagi pengguna yang berwenang.

## 2. Jenis Ancaman Siber

### 2.1 Malware

Malware adalah singkatan dari malicious software, yaitu perangkat lunak berbahaya yang dirancang untuk merusak, menginfeksi, atau mendapatkan akses tidak sah ke sistem komputer, jaringan, atau data. Malware dapat digunakan oleh penyerang untuk berbagai tujuan, seperti mencuri informasi pribadi, merusak data, mengontrol perangkat, atau memata-matai aktivitas pengguna. Berikut adalah Jenis-jenis Malware adalah :

a. Virus adalah Menempel pada program atau file, menyebar saat program dijalankan, dan dapat merusak sistem atau data.
b. Worm adalah Dapat menyebar sendiri melalui jaringan tanpa memerlukan interaksi pengguna, mengeksploitasi kerentanan perangkat lunak.
c. Trojan adalah Malware yang menyamar sebagai perangkat lunak sah, tetapi ketika dijalankan, membuka pintu bagi penyerang untuk mengakses sistem.
d. Ransomware adalah Mengenkripsi data korban dan meminta tebusan untuk mengembalikan akses ke data tersebut.
e. Spyware adalah Diam-diam memantau aktivitas pengguna dan mencuri informasi, seperti kata sandi atau data perbankan.
f. Adware adalah Menampilkan iklan yang tidak diinginkan, sering kali dengan tujuan mengganggu atau memanipulasi pengguna.

### 2.2 Phishing

Phishing adalah adalah salah satu bentuk serangan siber di mana penyerang mencoba untuk menipu korban agar memberikan informasi sensitif seperti kata sandi, nomor kartu kredit, atau informasi pribadi lainnya. Ini biasanya dilakukan dengan berpura-pura menjadi pihak yang sah, seperti bank, perusahaan, atau layanan online tepercaya, melalui komunikasi yang tampak

resmi, sering kali menggunakan email, pesan teks, atau situs web palsu. Jenis-jenis phising antara lain :

a. Spear Phishing adalah Serangan phishing yang ditargetkan pada individu atau organisasi tertentu, sering menggunakan informasi yang dipersonalisasi untuk membuat serangan lebih meyakinkan.
b. Whaling adalah Serangan phishing yang menargetkan eksekutif tinggi atau orang-orang berprofil tinggi dalam perusahaan, seperti CEO atau CFO.
c. Clone Phishing adalah Penyerang membuat salinan email asli tetapi memodifikasi konten atau tautan untuk menyisipkan malware atau mengarahkan korban ke situs palsu.
d. Smishing adalah Phishing yang dilakukan melalui pesan teks (SMS) dengan tautan atau permintaan yang mengarahkan korban ke situs web berbahaya.
e. Vishing adalah Phishing melalui panggilan telepon, di mana penyerang menyamar sebagai perwakilan dari institusi tepercaya untuk mencuri informasi pribadi.

**Contoh Kasus Phishing** Seorang penyerang dapat mengirimkan email yang tampak berasal dari bank pengguna, meminta mereka untuk "memverifikasi" akun mereka dengan mengklik tautan. Tautan tersebut mengarahkan korban ke situs web yang sangat mirip dengan situs asli bank, tetapi sebenarnya palsu, dan informasi yang dimasukkan pengguna (seperti username dan password) akan langsung jatuh ke tangan penyerang.

## 2.3 Serangan DoS (Denial of Service)

Denial of Service (DoS) adalah jenis serangan siber yang bertujuan untuk membuat layanan atau sumber daya jaringan, seperti situs web, server, atau jaringan, menjadi tidak dapat diakses oleh pengguna yang sah. Serangan DoS dilakukan dengan cara membanjiri target dengan lalu lintas yang berlebihan atau mengirimkan permintaan yang menyebabkan sumber daya sistem habis, sehingga server atau layanan tersebut gagal berfungsi. Serangan DoS bertujuan untuk membuat suatu layanan online tidak dapat digunakan dengan membanjiri jaringan atau server dengan trafik yang berlebihan.

Serangan DoS biasanya dilakukan dengan mengirimkan sejumlah besar permintaan palsu atau lalu lintas yang berlebihan ke server atau jaringan target. Karena sistem harus menangani semua permintaan yang masuk, sumber dayanya seperti CPU, RAM, dan bandwidth jaringan akan habis. Akibatnya, server atau layanan menjadi lambat atau sepenuhnya tidak dapat diakses oleh pengguna sah.

Jenis-jenis serangan DoS adalah sebagai berikut :

1. Flood Attack adalah Penyerang mengirimkan jumlah permintaan yang sangat besar ke server dengan kecepatan tinggi, melebihi kemampuan server untuk menanganinya. Contoh jenis flood attack termasuk:
    - UDP Flood adalah Mengirimkan paket UDP (User Datagram Protocol) dalam jumlah besar, membuat server sibuk memprosesnya.
    - ICMP Flood (Ping of Death) adalah Mengirimkan paket ping yang berlebihan ke server, menyebabkan overload pada server yang harus merespons permintaan tersebut.
2. SYN Flood adalah Mengirimkan sejumlah besar permintaan koneksi TCP dengan membuka sesi, tetapi tidak menyelesaikan proses "handshake" TCP. Hal ini membuat server menunggu jawaban yang tidak akan pernah datang, menghabiskan sumber daya hingga layanan menjadi tidak responsif.
3. Buffer Overflow Attack adalah Menyerang kelemahan perangkat lunak dengan mengirimkan data dalam jumlah yang jauh lebih besar daripada yang dapat ditangani oleh buffer sistem, sehingga menyebabkan crash atau malfungsi pada sistem.
4. Distributed Denial of Service (DDoS) adalah Serangan DoS yang lebih kompleks di mana serangan datang dari banyak perangkat yang terinfeksi (botnet) secara bersamaan, membuat serangan lebih sulit ditangkal karena volume lalu lintas yang jauh lebih besar. Botnet adalah jaringan komputer yang telah diretas dan dikendalikan oleh penyerang untuk mengirimkan serangan DDoS.

## 2.4 Serangan Man-in-the-Middle (MitM)

Serangan Man-in-the-Middle (MitM) adalah jenis serangan siber di mana penyerang diam-diam menyusup ke dalam komunikasi antara dua pihak yang berinteraksi secara digital (misalnya, dua perangkat atau antara pengguna dan

server). Penyerang bertindak sebagai perantara (man-in-the-middle) tanpa diketahui oleh kedua pihak, memungkinkan mereka untuk memata-matai, mencuri data sensitif, atau bahkan memodifikasi pesan yang ditransmisikan. Dalam serangan ini, penyerang mencegat komunikasi antara dua pihak tanpa diketahui, lalu mencuri atau memanipulasi data yang dikirimkan.

Serangan ini dapat terjadi di berbagai lapisan komunikasi, mulai dari jaringan Wi-Fi publik yang tidak aman hingga interaksi online yang melibatkan pertukaran data sensitif. Antara lain :

1. Penyadapan (Eavesdropping): Penyerang menyusup dan memantau komunikasi antara dua pihak tanpa mengubah isinya. Ini bisa digunakan untuk mencuri informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya.
2. Modifikasi Data (Tampering): Penyerang tidak hanya menyadap, tetapi juga mengubah pesan yang dikirim antara dua pihak. Misalnya, dalam transaksi keuangan, penyerang bisa mengubah detail transaksi sebelum diteruskan ke penerima.
3. Penyamaran (Impersonation): Penyerang menyamar sebagai salah satu pihak yang berkomunikasi dan memperdaya pihak lainnya agar berkomunikasi dengan penyerang, berpikir bahwa mereka berinteraksi dengan pihak asli.

Tahapan Serangan MitM diantaranya adalah :

1. Intersepsi (Interception) merupakan Penyerang pertama-tama harus mencegat komunikasi antara dua pihak. Ini bisa dilakukan dengan cara: Wi-Fi Publik yang Tidak Aman merupakan Penyerang dapat memanfaatkan jaringan Wi-Fi yang tidak aman atau mengatur jaringan palsu untuk menyusupkan diri ke dalam komunikasi.
2. DNS Spoofing merupakan Mengalihkan lalu lintas internet pengguna ke situs web palsu dengan memanipulasi pengaturan DNS.
3. ARP Spoofing merupakan Menyebabkan lalu lintas jaringan dialihkan melalui perangkat penyerang dengan memalsukan alamat ARP (Address Resolution Protocol).

Dalam beberapa kasus, jika komunikasi terenkripsi, penyerang harus men-dekripsi data agar bisa membaca atau memodifikasinya. Hal ini bisa terjadi dengan

serangan seperti SSL stripping, yang menurunkan koneksi aman HTTPS menjadi HTTP yang tidak aman. Dampak yang diakibatkan ddari Serangan MitM yaitu Pencurian Data Pribadi, Pengalihan Transaksi, Pencurian Identitas, Keamanan Komunikasi Rusak.

Contoh Kasus Serangan MitM yaitu Serangan Wi-Fi Publik Dimana Penyerang membuat hotspot Wi-Fi palsu di tempat umum, seperti kedai kopi atau bandara. Pengguna yang terhubung ke jaringan palsu ini mungkin berpikir bahwa mereka menggunakan Wi-Fi yang sah, tetapi semua data mereka disadap oleh penyerang dan Serangan pada Transaksi Keuangan Dimana Penyerang menyusup ke komunikasi antara pengguna dan situs perbankan, lalu mengubah detail transaksi (misalnya, mengganti nomor rekening penerima), sehingga uang dikirim ke akun penyerang.

## 2.5 Serangan Zero-day

Serangan Zero Day (Zero-Day Attack) adalah jenis serangan siber yang memanfaatkan kerentanan atau celah keamanan dalam perangkat lunak, perangkat keras, atau sistem yang belum diketahui atau belum diperbaiki oleh pengembang atau vendor. Istilah "zero-day" mengacu pada fakta bahwa pengembang memiliki nol hari untuk memperbaiki masalah karena celah keamanan tersebut belum diketahui atau belum diperbaiki sebelum serangan terjadi.

Serangan Zero Day Terjadi dikarenakan Penemuan Kerentanan suatu sistem dimana serangan Zero Day dimulai ketika penyerang menemukan celah keamanan atau kerentanan yang belum diketahui oleh pengembang perangkat lunak atau publik. Kerentanan ini bisa ada di sistem operasi, aplikasi, perangkat lunak keamanan, atau bahkan di perangkat keras. Selain itu, diakibatkan dari Pengembangan Eksploit dimana setelah menemukan kerentanan, penyerang membuat eksploitasi (exploit) khusus untuk memanfaatkannya. Eksploitasi ini bisa berupa malware, kode berbahaya, atau metode lain yang dapat memanipulasi celah keamanan tersebut. Yang terakhir adalah Eksploitasi vulnerability dimana

Eksploitasi zero day dapat digunakan untuk berbagai tujuan, seperti mencuri data, mengendalikan sistem, menyebarkan malware, atau merusak sistem target.

Berikut adalah ciri-ciri Serangan Zero Day adalah

1. Tidak Ada Patch yaitu Serangan terjadi sebelum vendor memiliki kesempatan untuk merilis patch atau perbaikan keamanan.
2. Tidak Terdeteksi oleh Sistem Keamanan Tradisional yaitu karena sifatnya yang belum dikenal, banyak sistem keamanan seperti antivirus atau firewall mungkin tidak mampu mendeteksi eksploitasi zero day.
3. Target Kerentanan Baru yaitu serangan biasanya menargetkan perangkat lunak atau sistem yang baru dirilis atau diupdate, karena versi baru sering kali memperkenalkan kerentanan yang belum diketahui.

Adapun Jenis-jenis dari Eksploitasi Zero Day adalah

1. Eksploitasi Aplikasi Web yaitu Serangan ini menargetkan aplikasi web atau layanan yang memiliki celah keamanan, seperti dalam kode JavaScript, SQL injection, atau cross-site scripting (XSS).
2. Eksploitasi Sistem Operasi yaitu Serangan zero day yang menargetkan sistem operasi (misalnya Windows, macOS, atau Linux), memanfaatkan celah dalam proses eksekusi, layanan jaringan, atau komponen inti sistem.
3. Eksploitasi Perangkat Lunak Pihak Ketiga yaitu Beberapa serangan zero day menargetkan aplikasi pihak ketiga yang umum digunakan seperti browser web, aplikasi kantor (misalnya Microsoft Office), atau plugin (misalnya Adobe Flash).
4. Eksploitasi Perangkat Keras yaitu Serangan zero day yang menargetkan kerentanan dalam perangkat keras atau firmware, seperti pada router, IoT (Internet of Things), atau komponen komputer lainnya.

Berikut daftar Contoh Serangan Zero Day yang paling terkenal, yaitu

1. **Stuxnet (2010).** Serangan malware canggih yang menargetkan sistem kontrol industri di Iran. Stuxnet mengeksploitasi beberapa kerentanan zero

day di Windows untuk menyebarkan malware ke sistem yang mengontrol sentrifugal nuklir. Serangan ini dianggap sebagai salah satu serangan siber paling signifikan dalam sejarah.

2. **Serangan Zero Day pada Internet Explorer (2014).** Eksploitasi zero day ditemukan di browser Internet Explorer, yang memungkinkan penyerang menjalankan kode berbahaya di komputer korban saat pengguna mengunjungi situs web berbahaya.
3. **WannaCry Ransomware (2017)** WannaCry memanfaatkan eksploitasi zero day yang dikenal sebagai "EternalBlue," yang menyerang kerentanan dalam protokol SMB (Server Message Block) pada sistem operasi Windows. Serangan ini menyebabkan kerugian besar di seluruh dunia, terutama pada jaringan infrastruktur penting seperti rumah sakit.

### 3. Cybercrime

Kejahatan dunia maya atau cyber crime adalah setiap kejahatan yang melibatkan komputer dan jaringan. Komputer mungkin telah digunakan untuk melakukan kejahatan, atau mungkin menjadi targetnya. Debatari Halder dan Dr. K. Jaishankar mendefinisikan Cybercrimes sebagai: "Pelanggaran yang dilakukan terhadap individu atau kelompok individu dengan motif kriminal untuk dengan sengaja merusak reputasi korban atau menyebabkan kerugian fisik atau mental, atau kerugian, kepada korban secara langsung atau secara tidak langsung, dengan menggunakan jaringan telekomunikasi modern seperti Internet seperti chatroom, email, papan pengumuman, grup dan telepon genggam (SMS/MMS)‖. Kejahatan semacam itu dapat mengancam keamanan dan kesehatan keuangan suatu negara. Isu seputar jenis kejahatan ini telah menjadi sorotan, terutama seputar peretasan, pelanggaran hak cipta, pornografi anak, dan perawatan anak. Ada juga masalah privasi ketika informasi rahasia dicegat atau diungkapkan, secara sah atau sebaliknya (Meeuwisse, 2015).

Secara internasional, baik aktor pemerintah maupun non-negara terlibat dalam kejahatan dunia maya, termasuk spionase, pencurian keuangan, dan kejahatan lintas batas lainnya. Kegiatan melintasi batas- batas internasional dan melibatkan kepentingan setidaknya satu negara bangsa kadang-kadang disebut sebagai cyberwarfare.

Forensik digital secara tradisional dikaitkan dengan investigasi kriminal dan, seperti yang Anda harapkan, sebagian besar jenis investigasi berpusat pada beberapa bentuk kejahatan komputer. Kejahatan semacam ini dapat mengambil dua bentuk; kejahatan berbasis komputer dan kejahatan yang difasilitasi komputer.

**6. Kesimpulan**

Cyber crime sudah dimulai sejak jaman dulu bahkan sebelum perkembangan internet begitu masif baik dari sisi penyebarannya ataupun kapasitas bandwidth-nya. Begitu maraknya perkembangan cyber crime dipicu oleh banyak faktor termasuk faktor ekonomi, faktor permusuhan, faktor ketenaran, faktor terorisme, faktor militer dan lain-lain. Dari semua faktor tersebut paling dominan adalah faktor ekonomi di mana cyber crime berorientasi pada keuntungan finansial bari penyerang.

Dalam satu dekade ini karena dipicu oleh perkembangan internet, pesatnya teknologi mobile seperti smartphone, ponsel, gadget, smartwatch, IoT maka perkembangan aplikasi yang berjalan di platform desktop, web ataupun mobile semakin banyak. Hal inilah yang juga menjadi pemicu maraknya cyber crime dengan berbagai macam modus, motif dan teknik yang semakin beragam. Aplikasi sosial media seperti Instagram, Tiktok, Facebook, Twitter dan Youtube semakin memicu maraknya cyber crime melalui sosial media. Ditambah lagi aplikasi messenger seperti WhatsApp, Telegram, Wechat di mana messenger ini memiliki jumlah pengguna berjumlah miliaran, sehingga memicu penyerang menggunakan sosial media dan messenger sebagai alat. Maraknya cyber crime telah terjadi hampir seluruh penjuru belahan dunia. Korbannya beraneka ragam dari institusi perbankan, institusi pendidikan, pemerintahan, swasta, bahkan perseorangan pun tidak lepas dari target serangan. Korban dari cyber crime tidak hanya kerusakan perangkat di beberapa kasus, namun sudah merugikan hampir ratusan triliun rupiah dampak kerugian yang ditimbulkan dari aksi serangan tersebut. Hal ini menjadi perhatian para ahli dan tentunya perlu penanganan lebih lanjut setelah terjadinya serangan yaitu dengan digital forensik untuk menginvestigasi kejadian cyber crime tersebut karena forensik di ranah cyber sangat berbeda dengan forensik di ranah kejahatan fisik. Digital forensik memerlukan alat dan software yang canggih dan terkini dalam melakukan investigasi dalam suatu kasus cyber crime.

Keamanan siber adalah tanggung jawab bersama. Dalam dunia yang semakin terkoneksi, ancaman terhadap data dan privasi meningkat, sehingga penerapan langkah-langkah keamanan yang kuat sangat penting. Modul ini memberikan gambaran umum tentang ancaman yang mungkin dihadapi serta cara-cara untuk melindungi diri dan organisasi dari serangan siber.