1. **CYBER SPACE**

 internet telah membentuk sebuah dunia tersendiri seperti layaknya bumi di tempat manusia berada. Dalam dunia maya ini, melalui teknologi informasi dan komunikasi, para individu maupun kelompok-kelompok masyarakat saling berinteraksi, bertukar pikiran, dan berkolaborasi untuk melakukan sejumlah aktivitas kehidupan.

1. **CYBER THREAT.**

Demikian pula hal yang sama menimpa internet. Semakin bertambah nilai dunia maya ini, semakin banyak pula ancaman yang menyertainya.

**3. CYBER ATTACK.**

jenis serangan di dunia maya dapat dikategorikan menjadi tiga jenis. Kategori pertama adalah kumpulan jenis serangan dimana teknologi informasi dan komunikasi menjadi alat atau senjata utama untuk melakukan kejahatan.

**4. CYBER SECURITY.**

Serangan yang cenderung bersifat destruktif tersebut sudah selayaknya harus ditangkal dan dihindari agar tidak merugikan banyak pihak.

**5. CYBER CRIME.**

jenis serangan yang terjadi di dunia maya. Jika dahulu diperkenalkan istilah hacker dan cracker yang menunjuk pada individu dengan kemampuan dan aktivitas khusus memasuki sistem komputer lain untuk beraneka ragam tujuan,

**6. CYBER LAW.**

menyusun dan memberlakukan undang-undang dunia maya (baca: cyber law). Dalam undang-undang ini biasanya disusun berbagai jenis klasifikasi dan ancaman hukuman terhadap beraneka ragam tindakan kriminal terkait dengan dunia komputer dan/atau teknologi informasi. Walaupun relatif terlambat dibandingkan dengan negara lain.

**Ekspoitasi keamanan**

1. Footprinting Mencari informasi terhadapa system-sistem untuk dijadikan sasaran, mencakup pencarian informasi dengan search engine, whois, dan DNS zone transfer.

2. Scanning Terhadap sasaran tertentu dicari pintu masuk yang paling memungkinkan dan mencari informasi IP menggunakan beberapa software.

3. Enumeration Intensif terhadap sasaran yang mencari user account abash, network resource and share, dan aplikasi untuk mendapatkan mana yang proteksinya lemah. 4. Gaining Acces Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran. Meliputi mengintip dan merampas password, menebak password serta melakukan buffer overflow.

5. Escalating Privilege Bila baru mendapatkan user password ditahap sebelumnya, ditahap ini diusahakan mendapat privilese admin jaringan dengan password cracking atau exploit sejenis getadmin, sechole, atau lc\_message.

6. Piltering Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke trusted system. Mencakup evaluasi trust dan pencarian cleartext password di registry, config file dan user data.

7. Covering Tracks Setelah control penuh terhadap system diperoleh, maka menutup jejak menjadi prioritas meliputi membersihkan network log dan penggunaan hide tool seperti macam-macam rootkit dan file streaming.

8. Creating Backdoors Diciptakan pada berbagai bagian dari system untuk memudahkan masuk kembali ke system ini dengan cara membentuk account palsu, menjadwalkan batch job, mengubah startup file, menanamkan servis pengendali jarak jauh serta monitoring tool, dan menggantikan aplikasi dengan Trojan.

9. Denial of Service Bila semua usaha di atas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir dengan berusaha mencegah pemakai yang sah untuk mengakses sebuah sumber daya tau informasi.

**Horizontal Privilage escalation**

Eskalasi hak akses horizontal adalah ketika pengguna mendapatkan akses hak pengguna lain yang memiliki tingkat akses yang sama dengannya melakukan.

mungkin bertanya-tanya mengapa seseorang ingin mendapatkan hak seseorang pada saat yang sama tingkat sebagai orang itu.

**Vertical Privilege Escalation**

Umumnya, ketika seseorang mencoba meretas sistem, itu karena mereka ingin melakukan beberapa tindakan pada sistem.

Dapat merusak sistem atau mencuri informasi.

Seringkali, ini membutuhkan tingkat hak akses yang tidak dimiliki penyerang sehingga bisa dimiliki.

Di sinilah eskalasi hak akses vertikal masuk.

Eskalasi hak akses vertikal adalah ketika penyerang menggunakan celah sistem untuk mendapatkan akses tersebut.

**ISO 27001** adalah standar audit berdasarkan persyaratan yang dapat diaudit, sedangkan **ISO 27002** adalah panduan implementasi berdasarkan saran praktik terbaik.

Untuk iso 27002 adalah seperangkat standar dan prosedur yang berkaitan. Dengan suatu keamanan dan kontrol informasi yang memungkinkan bisnis untuk menerapkan system keamanan yang tepat. Standar ini sebagian besar dilengkapi dengan iso 27001 yang bertugas untuk merinci manajerial seperti penilaian risiko dan meninjau keamanan. Di sisi lain iso 27002 banyak berbicara tentang aspek kontrol.

**Digital forensik**

**Menyikapi Kebocoran Data di Masa Pandemi**

pemerintah dan warga Indonesia dikagetkan dengan adanya temuan kebocoran data e-HAC pada tanggal akhir bulan Agustus 2021, pemerintah mengisyaratkan agar masyarakat Indonesia beralih pada aplikasi PeduliLindungi.

Pemerintah mengatakan bahwa data e-HAC pada aplikasi PeduliLindungi terjamin keamanannya karena berada pada pusat data nasional yang pengamanannya didukung kementerian dan lembaga terkait

Di Indonesia sendiri apabila kebocoran data tersebut dimanfaatkan oleh individu ataupun kelompok yang menjadikan celah tersebut untuk berbuat kejahatan atau yang biasa disebut cyber crime dengan memanfaatkan data-data individu warga negara Indonesia akan terjerat UU ITE alias Undang-undang Informasi dan Transaksi Elektronik.

Inilah yang menjadi tolak ukur akan pentingnya ahli forensik lebih tepatnya ahli forensik digital ataupun komputer forensik yang ahli pada kasus kejahatan dunia maya atau cyber crime.

**Strategi keamanan Akun Mail**

**SKENARIO EMAIL MUA DAN MTA**

**Standar mail**

Pemahaman fungsi dari masing-masing field itu dibutuhkan ketika kita akan melakukan forensic terhadap email, karena seringkali ada email palsu atau email-email ancaman.

* Setiap email memiliki kode Message-ID yang berbeda-beda (unik).
* Message-ID ini dibuat oleh MTA ketika dia mengirimkan email (yang pertama kali). Identitas ini dapat membantu kita dalam melakukan pelacakan.
* Sebagai contoh, kita bisa mencari (bertanya) apakah di berkas catatan (log) di server mail pengirim ada Message-ID tersebut.

SMTP merupakan protokol yang sederhana yang tidak memiliki pengamanan terhadap aspek penyadapan.

* Yang pertama, dari sisi pengguna, kita dapat melakukan enkripsi terhadap body email sehingga meskipun email kita disadap tetapi sang penyadap tidak dapat memperoleh isiny.
* Cara ini dapat dilakukan dengan mudah jika kita menggunakan PGP atau GPG.
* Cara yang lebih baik adalah dengan menggunakan protokol yang lebih aman.
* SMTPS, atau SMTP Secure, merupakan implementasi SMTP yang menggunakan enkripsi.
* Pada prinsipnya klien (MTA) tetap menggunakan protokol SMTP tetapi pada layer di bawahnya digunakan SSL atau TLS untuk menghindari penyadapan.
* SMTPS biasanya menggunakan port 587.