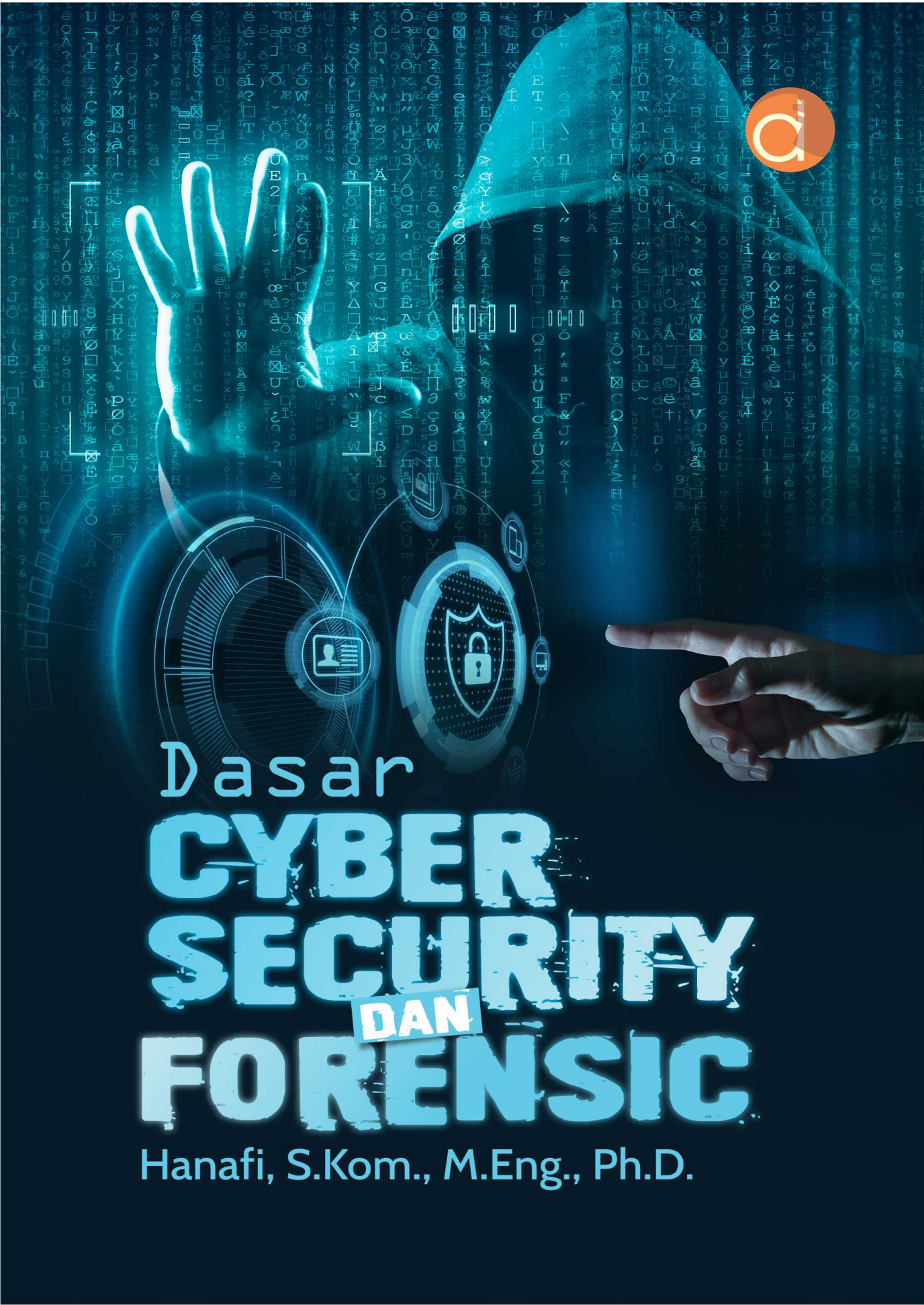


Dasar CYBER SECURITY DAN FORENSIC

Hanafi, S.Kom., M.Eng., Ph.D.

DASAR CYBER SECURITY
DAN FORENSIC

UU No 28 tahun 2014 tentang Hak Cipta

Fungsi dan sifat hak cipta Pasal 4

Hak Cipta sebagaimana dimaksud dalam Pasal 3 huruf a merupakan hak eksklusif yang terdiri atas hak moral dan hak ekonomi.

Pembatasan Pelindungan Pasal 26

Ketentuan sebagaimana dimaksud dalam Pasal 23, Pasal 24, dan Pasal 25 tidak berlaku terhadap:

i. Penggunaan kutipan singkat Ciptaan dan/atau produk Hak Terkait untuk pelaporan peristiwa aktual yang ditujukan hanya untuk keperluan penyediaan informasi aktual;
ii. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk kepentingan penelitian ilmu pengetahuan;
iii. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk keperluan pengajaran, kecuali pertunjukan dan Fonogram yang telah dilakukan Pengumuman sebagai bahan ajar; dan
iv. Penggunaan untuk kepentingan pendidikan dan pengembangan ilmu pengetahuan yang memungkinkan suatu Ciptaan dan/atau produk Hak Terkait dapat digunakan tanpa izin Pelaku Pertunjukan, Produser Fonogram, atau Lembaga Penyiaran.

Sanksi Pelanggaran Pasal 113

1. Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000 (seratus juta rupiah).
2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).

DASAR CYBER SECURITY DAN FORENSIC

Hanafi, S.Kom., M.Eng., Ph.D.

deepublish
Cerdas, Bahagia, Mulia, Lintas Generasi.

DASAR CYBER SECURITY DAN FORENSIC

Hanafi

Desain Cover :
Rulie Gunadi

Sumber :
ozrimoz (www.shutterstock.com)

Tata Letak :
G.D. Ayu

Proofreader :
Aditya Timor Eldian

Ukuran :
xviii, 236 hlm, Uk: 15.5x23 cm

ISBN :
978-623-02-5431-4

Cetakan Pertama :
November 2022

PENERBIT DEEPUBLISH
(Grup Penerbitan CV BUDI UTAMA)
Anggota IKAPI (076/DIY/2012)

Jl.Rajawali, G. Elang 6, No 3, Drono, Sardonoharjo, Ngaglik, Sleman
Jl.Kaliurang Km.9,3 – Yogyakarta 55581
Telp/Faks: (0274) 4533427
Website: www.deepublish.co.id
www.penerbitdeepublish.com
E-mail: cs@deepublish.co.id

KATA PENGANTAR

Bismillahirrahmanirrahim,

Puji syukur penulis panjatkan ke hadirat Allah Swt., yang telah memberikan kekuatan, kesabaran dan kesabaran sehingga buku yang sudah dipersiapkan ini akhirnya dapat diselesaikan.

Buku ini dipersiapkan untuk mahasiswa ilmu komputer atau khalayak umum yang sedang mempelajari teknologi *Cyber security*, karena sepanjang pengalaman penulis mengajar mata kuliah *Cyber security* sangat kurang literatur dalam bentuk buku sebagai buku pegangan mahasiswa.

Buku ini terdiri dari tiga bab pokok bagian, bab pertama berisi pengantar mengenai prinsip dasar serangan cyber, bab kedua mengenai teknologi yang mengubah jenis dan motif serangan, dan bab ketiga mengenai peluang dan tantangan *Cyber security*. terutama tentang *frame work*, pengujian keamanan, *digital forensic* dan *ethical hacking*.

Penulisan buku ini dimulai sejak tahun 2020 dalam catatan sederhana dan rangkuman bahan mengajar mata kuliah tentang *Cyber security*. Kemudian dilakukan perbaikan maupun peningkatan berkali-kali sehingga terbentuklah buku ini.

Penulis mengucapkan terima kasih kepada berbagai pihak yang telah membantu sehingga dapat diterbitkannya tulisan ini. penulis juga merasa bahwa buku ini jauh dari sempurna, oleh karena itu segala masukan baik berupa saran maupun kritik yang membangun sangat diharapkan.

Akhirnya semoga tulisan ini dapat bermanfaat bagi siapa saja yang ingin belajar dan mendalami tentang *Cyber security*.

Yogyakarta, 19 Oktober 2022

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

DASAR-DASAR *CYBER SECURITY*

1.1. Pendahuluan

Hampir semua industri dan kehidupan manusia menggunakan internet. Internet menjadi tulang punggung jalannya aplikasi yang digunakan oleh industri ataupun kehidupan manusia sehari-hari. Seperti kebutuhan akan energi dan pangan, internet juga menjadi kebutuhan dalam aktivitas kehidupan manusia. Internet terkoneksi dengan perangkat yang banyak digunakan oleh manusia seperti gadget, *handphone*, smartwatch, GPS, laptop ataupun PC. Dan semua alat tersebut terpasang berbagai aplikasi untuk membantu aktivitas kehidupan seperti belanja, transaksi perbankan, travelling, menulis dan lain sebagainya.

Di masa sekarang di mana dalam industri yang bergerak cepat ini, digitalisasi dan semua terhubung dengan internet. Ini lebih lanjut ditambah dengan proliferasi teknologi berbasis *cloud* dan seluler yang berkembang sangat pesat dalam dua dekade terakhir. Hal ini tentunya akan berdampak terhadap isu keamanan dalam kegiatan berinternet tentunya atau dalam diksi yang lebih tepat adalah *cyber security*. Apa pentingnya *cyber security*? Adalah pertanyaan yang telah beralih dari diskusi tim keamanan ke diskusi ruang dewan, dan tidak berhenti di situ juga. Ini, sekarang, adalah pembicaraan di industri saat ini. Setiap orang yang kita kenal di sekitar kita, di tempat kerja kita atau lainnya, berbicara tentang keamanan, dengan satu atau lain cara. Keamanan tidak lagi hanya menjadi kebutuhan administrator TI, atau administrator keamanan dalam organisasi TI. Sekarang persyaratan semua entitas yang terhubung dalam satu atau lain cara dengan semua jenis data.

1.2. Sejarah Kejahatan Cyber

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.

1.3. Motivasi dan Jenis Serangan

Terjadinya sekarang pada saat ini diyakini bahwa kita memiliki pemahaman tentang keamanan dan pentingnya sampai batas tertentu. Jadi, mari kita lihat apa itu permukaan serangan, dan bagaimana kita mendefinisikannya, karena penting untuk memahami permukaan serangan sehingga kita dapat merencanakan dengan baik untuk keamanan kita. Dalam istilah yang sangat sederhana, permukaan serangan adalah kumpulan semua kerentanan potensial yang, jika dieksploitasi, dapat memungkinkan akses tidak sah ke sistem, data, atau jaringan. Kerentanan ini sering juga disebut vektor serangan, dan mereka dapat menjangkau dari

perangkat lunak, perangkat keras, jaringan, dan pengguna yang merupakan faktor manusia. Risiko diserang atau dikompromikan berbanding lurus dengan tingkat paparan permukaan serangan. Semakin tinggi jumlah vektor serangan, semakin besar permukaan serangan, dan semakin tinggi risiko kompromi. Jadi, untuk mengurangi risiko serangan, seseorang perlu mengurangi permukaan serangan dengan mengurangi jumlah vektor serangan.

Kami menyaksikan setiap saat yang menyerang aplikasi target, infrastruktur jaringan, dan bahkan individu. Hanya untuk memberi kita tingkat permukaan serangan dan eksposur, mari kita lihat *database* Common Vulnerabilities and Exposure (CVE) (https://cve.mitre.org/cv e/). Ini memiliki 108.915 entri CVE (pada saat penulisan bab ini), yang semuanya telah diidentifikasi sejauh ini selama beberapa dekade terakhir. Tentu banyak dari ini sekarang diperbaiki, tetapi beberapa mungkin masih ada. Angka yang sangat besar ini menunjukkan seberapa besar risiko paparannya.

Perangkat lunak apa pun yang berjalan dalam suatu sistem berpotensi dieksploitasi menggunakan kerentanan dalam perangkat lunak, dari jarak jauh atau lokal. Ini berlaku terutama untuk perangkat lunak yang menghadap ke web, karena lebih terbuka, dan permukaan serangannya jauh lebih besar. Seringkali, aplikasi dan perangkat lunak yang rentan ini dapat menyebabkan kompromi seluruh jaringan, dan juga menimbulkan risiko pada data yang dikelolanya. Terlepas dari ini, ada risiko lain bahwa aplikasi atau perangkat lunak ini terpapar sepanjang waktu: ancaman orang dalam, di mana setiap pengguna yang diautentikasi dapat memperoleh akses ke data yang tidak terlindungi karena kontrol akses yang diterapkan dengan buruk.

Di sisi lain, permukaan serangan yang mengekspos serangan jaringan bisa pasif atau aktif. Permukaan serangan ini dapat membuat layanan jaringan runtuh, membuatnya tidak tersedia untuk sementara, memungkinkan akses tidak sah dari data yang mengalir melalui jaringan, dan sebagainya. Jika terjadi serangan pasif, jaringan dapat dipantau oleh musuh untuk menangkap kata sandi, atau untuk menangkap informasi yang bersifat sensitif. Selama serangan pasif, seseorang dapat memanfaatkan lalu lintas jaringan untuk mencegat komunikasi antara

sistem sensitif dan mencuri informasi. Ini dapat dilakukan tanpa pengguna mengetahuinya. Sebagai alternatif, selama serangan aktif, musuh akan mencoba untuk melewati sistem perlindungan dengan menggunakan malware atau bentuk lain dari kerentanan berbasis jaringan untuk membobol aset jaringan; serangan aktif dapat menyebabkan paparan data dan file sensitif. Serangan aktif juga dapat menyebabkan serangan tipe Denial-of-Service.

Peta ancaman dapat didefinisikan sebagai kumpulan ancaman yang diamati, informasi tentang agen ancaman, dan tren ancaman saat ini. Penting bagi setiap profesional keamanan untuk melacak lanskap ancaman. Biasanya, banyak lembaga dan vendor keamanan yang berbeda akan merilis laporan lanskap ancaman seperti itu, misalnya, ENISA (European Union Agency for Cybersecurity), dan NIST (National Institute of Standards and Technology), bersama dengan beberapa perusahaan keamanan besar.

Selain itu, lanskap ancaman adalah ruang yang sangat dinamis; itu sangat sering berubah, dan didorong oleh banyak faktor, seperti alat yang tersedia untuk mengeksploitasi kerentanan, basis pengetahuan sumber daya dan kerentanan yang tersedia, dan persyaratan keterampilan untuk melakukan serangan. Ini menjadi semakin mudah karena alat yang tersedia secara bebas di internet. Kami akan berbicara lebih banyak tentang sumber daya lanskap ancaman dalam bab-bab berikutnya dalam buku ini. Berikut ini adalah daftar berbagai ancaman di tahun 2016-2019 dan peringkat relatifnya:

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware		1. Malware		→
2. Web Based Attacks		2. Web Based Attacks		→
3. Web Application Attacks		3. Web Application Attacks		→
4. Phishing		4. Phishing		→
5. Spam		5. Denial of Service		↑
6. Denial of Service		6. Spam		↓
7. Ransomware		7. Botnets		↑
8. Botnets		8. Data Breaches		↑
9. Insider threat		9. Insider Threat		→
10. Physical manipulation/ damage/ theft/loss		10. Physical manipulation/ damage/ theft/loss		→
11. Data Breaches		11. Information Leakage		↑
12. Identity Theft		12. Identity Theft		→
13. Information Leakage		13. Cryptojacking		NEW
14. Exploit Kits		14. Ransomware		↓
15. Cyber Espionage		15. Cyber Espionage		→

Gambar 1.1 Peta serangan *cyber*

Gambar 1.1 adalah peta serangan yang berkembang sampai dengan tahun 2017 berdasarkan laporan dari ENISA. Ini membawa kita ke titik di mana penting untuk mengetahui sedikit tentang beberapa jenis serangan yang akan dijabarkan pada sesi berikut ini.

1.3.1. Serangan tidak terstruktur

Ini adalah salah satu serangan di mana musuh 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.

1.3.2. 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.

1.3.3. Rekayasa sosial (Phishing, Spear phishing)

Serangan ini ditargetkan ke salah satu tautan terlemah, manusia. Dalam serangan ini, pengguna dieksploitasi dengan berbagai cara. Seringkali serangan ini berhasil karena kurangnya pengetahuan atau ketidaktahuan. Informasi diekstraksi dari pengguna dengan menipu mereka dengan satu atau lain cara. Cara yang paling umum adalah dengan *phishing* dan *spear phishing*. Dalam serangan *phishing* dan *spear phishing*, data diekstraksi dengan meniru sesuatu yang terlihat asli bagi pengguna, seperti, menyamar sebagai administrator yang membantu pengguna untuk mengatur ulang kata sandi mereka, dan detail akun lainnya, melalui *port*al web. *Port*al ini dibuat secara khusus agar sesuai dengan tujuan mengekstraksi data yang ingin dikumpulkan oleh penyerang. Pengguna menjadi mangsa mereka, dan berbagi informasi sensitif. Menguping: Serangan ini dapat dilakukan dengan mendapatkan akses tidak sah ke jaringan dan mendengarkan komunikasi jaringan. Umumnya, semua lalu lintas yang tidak dienkripsi dapat dengan mudah ditargetkan oleh penyerang.

1.3.4. Denial of Service (DoS dan DDoS)

Ini adalah salah satu bentuk serangan berbasis jaringan tertua, di mana penyerang akan mencoba untuk membanjiri kapasitas pemrosesan atau komputasi aplikasi atau perangkat dengan mengirimkan banjir data yang melebihi yang dapat ditangani oleh aplikasi atau perangkat, sehingga mengganggu sistem. Di sisi lain, Deniel of Service (DDoS), diluncurkan dari berbagai sumber menuju aplikasi atau sistem korban tunggal dalam

skala yang sangat besar, lebih dari jumlah yang dapat ditangani. Ini adalah salah satu yang paling sulit untuk dikurangi tanpa teknologi yang tepat.

1.3.5. Man-in-the-middle attack (MITM)

Dalam bentuk serangan ini, sesi atau jaringan dibajak di antaranya dengan memanipulasi komunikasi antara server dan klien, dan bertindak sebagai server *proxy*, seringkali tanpa sepengetahuan korban. Malware: Malware dapat didefinisikan sebagai perangkat lunak pengganggu, yang sengaja dirancang untuk menyebabkan kerusakan atau mencapai maksud jahat lainnya oleh penciptanya. Sebagian besar waktu, akses ini diperoleh dengan mengeksploitasi keamanan sistem komputasi, atau kerentanan apa pun, dengan bantuan malware. Worms dan Trojans adalah bentuk malware yang berbeda, dan ini memiliki kemampuan yang sangat spesifik untuk menyebar dari komputer ke komputer dan mereplikasi diri mereka sendiri. Malware dapat menyebabkan pencurian data, pemusnahan massal sistem komputer, gangguan aktivitas jaringan, dan juga dapat membantu dalam spionase perusahaan. Sebagian besar malware terbaru mungkin memiliki kemampuan unik untuk menyembunyikan dirinya dengan sangat baik dari sistem keamanan dan mekanisme deteksi, dan tetap aktif selama berminggu-minggu hingga bertahun-tahun.

1.3.6. Botnet

Ketika sistem komputer terinfeksi malware, atau alat jarak jauh berbahaya lainnya, dan sistem komputer yang terinfeksi ini dikendalikan oleh penyerang dari jarak jauh, itu dikenal sebagai bot. Selain itu, ketika ada banyak komputer yang disusupi oleh malware ini, dan dikendalikan oleh penyerang, jaringan ini, atau kumpulan komputer yang disusupi, disebut botnet. Mekanisme jarak jauh dan metode kontrol juga disebut sebagai "Perintah dan Kontrol". Botnet dapat digunakan untuk berbagai tujuan lain oleh musuh, dan untuk mencapainya, master botnet akan terus memperbarui biner program jahat. Botnet dulunya hanya berfokus pada satu hal misi. Namun, di masa lalu, mereka telah berubah menjadi aplikasi berbahaya multiguna.

1.3.7. Skrip lintas situs

Skrip lintas situs, umumnya dikenal sebagai serangan XSS, adalah eksploitasi kelemahan dalam aplikasi web, yang memungkinkan musuh menyuntikkan skrip sisi klien yang berbahaya dan membahayakan pengguna, tanpa sepengetahuan mereka dalam banyak kasus. Secara umum, kekurangan ini ada karena validasi input yang buruk dari aplikasi berbasis web. Setelah XSS dikirim ke pengguna, browser akan memprosesnya karena browser tidak memiliki mekanisme untuk menghentikan serangan berbasis XSS. Ada beberapa bentuk serangan XSS. Jenis XSS yang disimpan dan direfleksikan sangat umum. Disimpan XSS memungkinkan penyerang untuk meninggalkan skrip berbahaya permanen di server korban, sementara XSS yang direfleksikan biasanya terjadi ketika penyerang mengirimkan tautan yang dibuat khusus dengan kueri jahat di URL kepada pengguna, dan pengguna yang tidak curiga mengklik tautan tersebut, yang kemudian membawa pengguna ke situs berbahaya dan menangkap data sensitif pengguna, yang kemudian dikirim ke penyerang. XSS yang direfleksikan hanya mungkin jika pengguna mengklik tautan. Atau, metode lain adalah jika penyerang mengelabui pengguna agar mengkliknya.

1.3.8. Serangan download drive-by

Bentuk serangan ini sangat umum terlihat melalui internet. Ini telah menjadi salah satu ancaman utama dalam beberapa tahun terakhir. Dalam praktiknya, penyerang akan berkompromi dengan situs web jinak yang terkenal dan meng-*hosting* malware mereka di sana, dengan menyematkan tautan berbahaya. Setelah pengguna mengunjungi situs web yang tidak mencurigakan ini, mereka dikompromikan dengan secara otomatis dialihkan ke lokasi unduhan malware. Seringkali, tautan situs web yang disusupi dapat disebarkan melalui email spam atau *phishing*, di mana pengguna mungkin mengeklik tautan karena penasaran, atau tanpa sadar, dan mengunduh malware ke dalam sistem. Serangan injeksi SQL yaitu Serangan injeksi SQL biasanya ditargetkan ke *database* yang diekspos melalui web. Penyerang akan mengeksekusi kueri berbahaya melalui aplikasi web yang dikonfigurasi dengan buruk, sebagian besar dalam

mekanisme input data untuk menjalankan perintah SQL. Penyerang, jika berhasil, dapat memperoleh akses ke *database*, memanipulasi data sensitif, atau, kadang-kadang, juga memodifikasi data. Injeksi SQL juga dapat memungkinkan perintah sewenang-wenang untuk mengelola sistem operasi dari jarak jauh. Kerentanan ini sebagian besar berhasil karena sanitasi masukan yang buruk di aplikasi web, bukan di akhir basis data, karena basis data dirancang untuk mengeksekusi kueri saat menerimanya dan mengembalikan hasil yang sesuai. Jadi, pengembang harus berhati-hati dengan sanitasi input dan hanya menerima input data sesuai keinginan, dan memeriksa setiap input berbahaya, sebelum mengirimkannya ke *database* untuk eksekusi kueri.

1.3.9. Advanced Persistent Threat (APT)

Serangan ini telah meningkat selama bertahun-tahun. Modus operandi serangan ini sebagian besar untuk meluncurkan serangan yang sangat bertarget terhadap organisasi individu tertentu, segmen industri, atau bahkan suatu negara. Ancaman ini disebut "persisten lanjutan" karena penyerang, atau kelompok penyerang, akan menggunakan banyak teknik canggih dan tersembunyi untuk tetap tidak terdeteksi untuk waktu yang sangat lama. Seringkali, ditemukan bahwa serangan dan metode persisten secara khusus dibuat untuk serangan tertentu dan tidak pernah digunakan dalam serangan lain. Serangan berbasis APT sebagian besar didanai dengan baik dan sebagian besar merupakan aktivitas yang digerakkan oleh tim. APT digunakan untuk menargetkan kekayaan intelektual, segala bentuk informasi sensitif, aktivitas yang mengganggu, atau bahkan mungkin untuk spionase perusahaan, atau sabotase data, dan/atau infrastruktur. Serangan APT sama sekali berbeda dari bentuk serangan lainnya; musuh/musuh mengambil pendekatan yang sangat terorganisir untuk mengetahui target mereka dan misi yang ingin mereka capai, dan mereka tidak terburu-buru untuk menyerang. Infrastruktur serangan terkadang sangat kompleks. Tujuan utama penyerang/penyerang adalah untuk tetap berada di jaringan yang disusupi selama mungkin dan tetap tersembunyi dari deteksi keamanan. Salah satu sifat penting dari APT, adalah bahwa hal itu hanya dapat mempengaruhi bagian-bagian tertentu dari jaringan, atau orang-orang tertentu dalam perusahaan, atau hanya

beberapa sistem dalam jaringan yang menjadi *point of interest*. Oleh karena itu, lebih sulit untuk mendeteksi aktivitas APT oleh sistem pemantauan keamanan.

1.3.10. Serangan Basis Web

Dalam serangan ini, seperti namanya, sistem target sebagian besar adalah perangkat yang menghadap internet, aplikasi, layanan, dan sebagainya. Praktis, kita bisa mengatakan bahwa sebagian besar aplikasi internet terkena serangan web. Ini dapat diserang melalui kelemahan dan kerentanan, tidak hanya di aplikasi, tetapi juga di media yang kami gunakan untuk mengakses aplikasi tersebut, seperti browser web. Eksploitasi browser web telah meningkat selama bertahun-tahun. Server web selalu menjadi target yang sangat menguntungkan bagi musuh/musuh. Beberapa bentuk serangan yang terkenal adalah unduhan *drive-by* atau serangan lubang air (di mana aplikasi web yang sah, yang digunakan oleh target/organisasi yang ditargetkan, dikompromikan dan kemudian penyerang menunggu karyawan/pengguna mengunjungi situs web dan, dengan demikian, itu menjadi terganggu).

1.3.11. Serangan dari Internal

Serangan orang dalam adalah elemen manusia dari keamanan siber yang sangat rentan dan sangat sulit untuk dilacak, dipantau, dan dimitigasi. Ancaman ini menunjukkan bahwa pengguna dengan akses resmi ke aset informasi akan menyebabkan kerugian bagi entitas/bisnis, atau organisasi. Hal ini terkadang dilakukan tanpa disadari dengan menjadi mangsa, atau terkadang merekalah yang melakukan serangan. Secara umum, tidak ada cara pasti untuk mendeteksi atau memantau ancaman orang dalam secara proaktif; itu hanya dapat ditemukan ketika kerusakan telah terjadi di mkasus ost. Ini telah menjadi tren yang meningkat selama bertahun-tahun, karena penyerang tingkat lanjut mencoba mengeksploitasi orang dalam untuk mendapatkan akses ke organisasi atau bisnis. Ini telah menjadi ancaman besar bagi pemerintah dan semakin meningkat dari hari ke hari. Bahkan jika organisasi memiliki jaringan anti peluru dengan lingkungan yang terkunci, dan pertahanan perimeter yang kuat, serangan orang dalam

dianggap yang paling efektif. Mitigasi ancaman orang dalam berada di luar implementasi teknis. Organisasi juga perlu memasukkan budaya sosial dan pendidikan penggunanya sendiri tentang bagaimana memperlakukan keamanan dan tetap waspada.

1.3.12. Ransomware

Ransomware telah melakukan banyak kerusakan baru-baru ini dan telah muncul sebagai ancaman yang menonjol. Modus operandi ransomware sebagian besar untuk mendapatkan keuntungan moneter dengan menahan data/sistem pengguna dalam tebusan dengan membuatnya tidak dapat digunakan. Ini dicapai dengan mengkompromikan sistem dengan satu atau bentuk lain dari eksploitasi dan kerentanan yang ada dan kemudian mengenkripsi data dalam sistem pengguna. Setelah dienkripsi, penyerang akan meminta uang sebagai ganti kunci deskripsi.

1.3.13. Spionase

Ini adalah salah satu masalah serius yang selalu ada sejak awal perang manusia. Saat ini, ini terjadi antara perusahaan, pemerintah, dan berbagai entitas lainnya, dan medan pertempurannya adalah dunia maya. Ini menguntungkan, dalam arti tertentu, karena tidak ada yang langsung datang ke depan untuk melakukan spionase ini; mereka semua berada di balik dunia maya yang tersembunyi, dan penyerang dapat tetap anonim. Kita telah melihat dalam berita dalam beberapa tahun terakhir bagaimana satu pemerintah mencoba untuk merusak atau mengganggu yang lain dengan menggunakan bentuk spionase dunia maya, dengan mengkompromikan informasi sensitif, dan kemudian membocorkannya ke publik, untuk menyebabkan kekacauan dan gangguan. Bahkan perusahaan tidak jauh di belakang. Mereka melakukannya untuk mendapatkan akses ke kekayaan intelektual masing-masing untuk tetap menjadi yang terdepan dalam persaingan. Dunia maya jauh lebih menarik dan berbahaya jika kita berpikir dari perspektif keamanan siber ini.

1.4. Digital Forensic

Forensik digital adalah seni memulihkan dan menganalisis konten yang ditemukan pada perangkat digital seperti desktop, notebook/netbook, tablet, smartphone, dll, tidak banyak diketahui selama beberapa tahun yang lalu. Namun, dengan meningkatnya insiden kejahatan dunia maya, dan meningkatnya adopsi perangkat digital, cabang forensik ini menjadi sangat penting belakangan ini, menambah apa yang secara konvensional terbatas pada pemulihan dan analisis biologis dan bukti kimia selama investigasi kriminal.

1.4.1. Definisi komputer forensik

Forensik komputer adalah praktik mengumpulkan, menganalisis, dan melaporkan data digital dengan cara yang dapat diterima secara hukum. Ini dapat digunakan dalam deteksi dan pencegahan kejahatan dan dalam perselisihan apa pun di mana bukti disimpan secara digital. Ini adalah penggunaan teknik khusus untuk pemulihan, autentikasi dan analisis data elektronik ketika sebuah kasus melibatkan masalah yang berkaitan dengan rekonstruksi penggunaan komputer, pemeriksaan data sisa, dan autentikasi data dengan analisis teknis atau penjelasan fitur teknis data dan penggunaan komputer. Forensik komputer memerlukan keahlian khusus yang melampaui pengumpulan data normal dan teknik penjagaan yang tersedia untuk pengguna akhir atau personel pendukung sistem. Mirip dengan semua bentuk ilmu forensik, forensik komputer terdiri dari penerapan hukum pada ilmu komputer. Forensik komputer berkaitan dengan pelestarian, identifikasi, ekstraksi, dan dokumentasi bukti komputer. Seperti banyak ilmu forensik lainnya, forensik komputer melibatkan penggunaan alat dan prosedur teknologi canggih yang harus diikuti untuk menjamin keakuratan pelestarian bukti dan keakuratan hasil mengenai pemrosesan bukti komputer. Penggunaan teknik khusus untuk pemulihan, autentikasi, dan analisis data komputer, biasanya data yang mungkin telah dihapus atau dihancurkan.

1.4.2. Cyber crime

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.

1.5. 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*.

1.6. Latihan

1. Sebutkan jenis serangan siber yang sering terjadi di Indonesia yang menyebabkan kerugian terbesar baik untuk masyarakat atau negara!
2. Situs pemerintah sering dijadikan ajang untuk kejahatan cyber, upaya apa yang sebaiknya dilakukan untuk mengurangi risiko pada aspek tersebut?
3. Motif apa saja yang melatarbelakangi serangan siber yang terjadi pada situs pemerintah?

4. Lembaga swasta maupun pemerintah kurang memberikan perhatian yang serius pada aspek *cyber security*, apa yang menyebabkan hal tersebut terjadi dan apa upaya yang sebaiknya dilakukan untuk mengantisipasi hal tersebut?
5. Kejahatan siber selalu meningkat dari tahun ke tahun dengan modus yang tambah beragam, faktor apa saja yang menyebabkan hal itu terjadi?

BAB II

FRAMEWORK CYBER SECURITY

2.1. Pendahuluan

2.1.1. Dasar keamanan informasi

Ada tiga faktor penting dalam mencapai *cyber security* yang selayaknya dicapai yaitu autentikasi, otorisasi, dan *nonrepudiation* di mana ketiga hal itu adalah alat yang dapat digunakan oleh perancang sistem untuk menjaga keamanan sistem sehubungan dengan kerahasiaan, integritas, dan ketersediaan. Memahami masing-masing dari enam konsep ini dan bagaimana mereka berhubungan satu sama lain membantu profesional keamanan merancang dan mengimplementasikan sistem yang aman. Setiap komponen sangat penting untuk keamanan keseluruhan, dengan kegagalan salah satu komponen yang mengakibatkan potensi kompromi sistem.

Gambar 2.1 Ilustrasi triad *cyber security*

Dalam pemahaman umum sebagai upaya mencapai sistem keamanan yang ideal, ada tiga konsep kunci penting yang dikenal sebagai triad CIA yang merupakan kepanjangan dari segitiga [C] *confidentiality*, [I] *integrity*, [A] *availability*, di mana hal ini harus dipahami oleh siapa pun yang melindungi sistem informasi: *confidentiality* yang mengacu pada makna kerahasiaan, integritas lebih mengacu pada makna integritas, dan *availability* yang mengacu pada makna ketersediaan. Perancangan keamanan informasi yang kredibel selayaknya untuk memastikan prinsip perlindungan ini untuk setiap sistem yang mereka aplikasikan. Selain itu, ada tiga konsep utama yang harus dipahami oleh para praktisi dan profesional keamanan untuk menegakkan prinsip-prinsip CIA dengan benar yaitu meliputi tiga aspek penting: autentikasi, otorisasi, dan nonrepudiasi. Pada sub bab di bawah akan dijelaskan masing-masing konsep ini dan bagaimana mereka berhubungan satu sama lain di bidang keamanan digital. Semua definisi yang digunakan dalam bagian ini berasal dari National Information Assurance Glossary (NIAG) yang diterbitkan Komite Sistem Keamanan Nasional AS yang secara resmi dibentuk oleh pemerintahan Federal Amerika Serikat.

2.1.1.1. Autentikasi

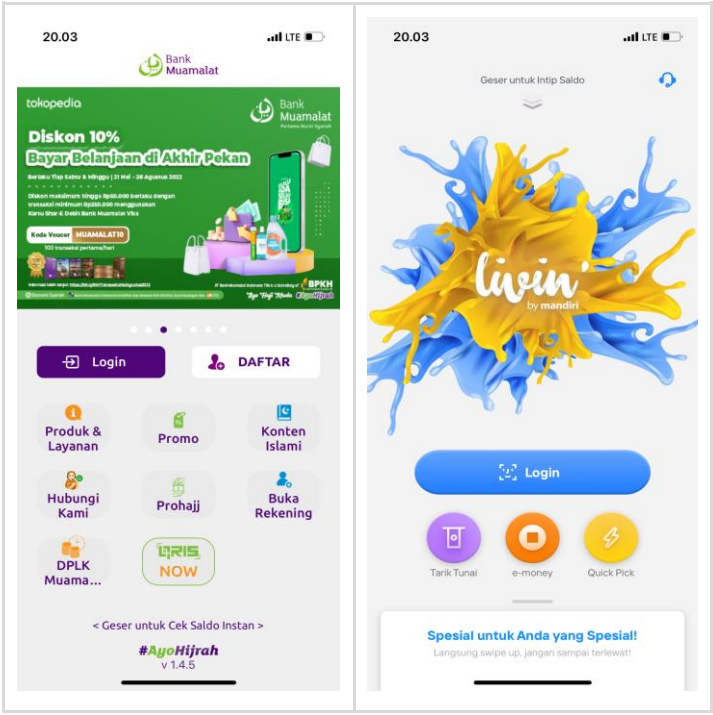
Autentikasi merupakan hal penting untuk sistem keamanan apa pun, karena itu adalah kunci untuk memverifikasi sumber pesan atau bahwa seseorang adalah siapa yang dia klaim. NIAG mendefinisikan autentikasi sebagai ukuran keamanan yang dirancang untuk menetapkan validitas transmisi, pesan, atau pencetus, atau sarana untuk memverifikasi otorisasi individu untuk menerima kategori informasi tertentu.

Tabel 2.1 Beberapa aspek yang penting untuk autentikasi keamanan

Sesuatu yang Anda Ketahui	Informasi yang diasumsikan sistem tidak diketahui orang lain; informasi ini mungkin rahasia, seperti kata sandi atau kode PIN, atau hanya sepotong informasi yang kebanyakan orang tidak tahu, seperti nama gadis ibu pengguna.
Sesuatu yang Anda Miliki	Sesuatu yang dimiliki pengguna yang hanya dia miliki; lencana Radio Frequency ID (RFID), *One-Time-Password* (OTP) yang menghasilkan Token, kata sandi, atau kunci fisik
Sesuatu yang Anda miliki	Sidik jari seseorang, pemindaian wajah, pemindaian tubuh, cetakan suara, atau pemindaian retina atau elemen yang dikenal sebagai fitur biometrik

Dalam aplikasi sehari-hari telah dicontohkan banyak model autentikasi seperti yang paling umum ketika kita membuka email maka akan diminta memasukan *password*, ketika kita akan bertransaksi keuangan melalui *mobile banking* atau *payment gateway* maka perlu dua lapis yaitu *password* dan pin, ketika kita akan masuk suatu ruangan yang penting maka perlu memasukan *finger print* atau *id card*, dan masih banyak lagi contoh dalam aplikasi sehari-hari.

Ada banyak metode yang tersedia untuk mengautentikasi seseorang. Dalam setiap metode, autentikator mengeluarkan tantangan yang harus dijawab seseorang. Tantangan ini biasanya terdiri dari permintaan informasi yang hanya dapat diberikan oleh pengguna asli. Potongan informasi ini biasanya masuk ke dalam tiga klasifikasi yang dikenal sebagai faktor autentikasi.



Gambar 2.2 Tampilan layar bentuk autentikasi pada beberapa bank nasional Indonesia

Ketika sistem autentikasi membutuhkan lebih dari satu faktor ini, komunitas keamanan mengklasifikasikannya sebagai sistem yang membutuhkan autentikasi multifaktor. Dua contoh dari faktor yang sama, seperti kata sandi yang digabungkan dengan nama gadis ibu pengguna, bukanlah autentikasi multifaktor, tetapi menggabungkan pemindaian sidik jari dan nomor identifikasi pribadi (PIN) adalah karena memvalidasi sesuatu yang dimiliki pengguna pemilik sidik jari itu dan sesuatu yang diketahui pengguna PIN.

Di hampir semua layanan yang membutuhkan keamanan tertinggi seperti perbankan membutuhkan beberapa *layer* autentikasi. Hal ini dilakukan akan kejahatan di bidang perbankan seperti pengalihan dana, pencurian deposito, pengambilan dana nasabah tidak akan terjadi. Perbankan menerapkan autentikasi berlapis seperti menggunakan *password* untuk masuk ke app, namun ada juga yang memerlukan *scan*

wajah, *scan* retina, *finger print* dan lain-lain. Selanjutnya diperlukan pin untuk melakukan transaksi keuangan seperti memeriksa jumlah rekening, transfer uang ke rekening lain.

Dalam beberapa kasus di negara kita Indonesia dalam registrasi E-KTP juga diperlukan pengambilan data yang bersumber dari retina mata, kita ketahui bersama bahwa dalam retina mata terhadap karakter yang unik pada setiap manusia seperti juga pada *finger* manusia. Retina mata juga dapat digunakan sebagai informasi untuk autentikasi. Di era modern ini sudah tersedia alat yang diciptakan para fabrikan untuk *scanning* retina mata dengan sangat mudah. Beberapa aplikasi penggunaan deteksi retina mata seperti untuk masuk ke ruangan yang membutuhkan keamanan tinggi seperti ruang data center, ruang penyimpanan barang-barang berharga. Penggunaan anggota tubuh seperti postur tubuh, jempol tangan, retina mata, pola wajah sering dikenal dengan biometrik. Ke depan teknologi akan menjadi tren dalam mengautentikasi dalam upaya meningkatkan keamanan sistem.

Autentikasi juga berlaku untuk memvalidasi sumber pesan, seperti paket jaringan atau email. Pada tingkat rendah, sistem autentikasi pesan tidak dapat mengandalkan faktor yang sama yang berlaku untuk autentikasi manusia. Sistem autentikasi pesan sering mengandalkan tanda tangan kriptografis, yang terdiri dari intisari atau hash dari pesan yang dihasilkan dengan kunci rahasia. Karena hanya satu orang yang memiliki akses ke kunci yang menghasilkan tanda tangan, penerima dapat memvalidasi pengirim pesan. Tanpa sistem autentikasi suara, tidak mungkin untuk mempercayai bahwa pengguna adalah siapa yang dia katakan, atau bahwa pesan berasal dari siapa yang diklaimnya.

2.1.1.2. Otorisasi

Otorisasi secara umum mempunyai makna orang yang diberi izin atau kekuasaan. Berbeda dengan autentikasi berhubungan dengan verifikasi identitas, otorisasi berfokus pada penentuan apa yang izin untuk dilakukan oleh pengguna. NIAG mendefinisikan otorisasi sebagai “hak akses yang diberikan kepada pengguna, program, atau proses.” Setelah sistem yang aman mengautentikasi pengguna, ia juga harus memutuskan hak istimewa apa yang mereka miliki. Misalnya, aplikasi perbankan online akan

mengautentikasi pengguna berdasarkan kredensialnya, tetapi kemudian harus menentukan akun yang dapat diakses pengguna tersebut. Selain itu, sistem menentukan tindakan apa yang dapat dilakukan pengguna terkait akun tersebut, seperti melihat saldo dan melakukan transfer.

2.1.1.3. Nonrepudiation

Bayangkan sebuah skenario di mana Budi membeli mobil dari Agung dan menandatangani kontrak yang menyatakan bahwa dia akan membayar Rp. 2 Miliar untuk rumah tersebut dan akan mengambil alih kepemilikannya pada hari senin di mana transaksi itu ditanda tangani. Jika Budi kemudian memutuskan untuk tidak membeli rumah itu, dia mungkin mengklaim bahwa seseorang memalsukan tanda tangannya dan bahwa dia tidak bertanggung jawab atas kontrak tersebut. Untuk membantah klaimnya, Agung dapat menunjukkan bahwa notaris memverifikasi identitas Budi dan membubuhkan stempel pada dokumen untuk menunjukkan verifikasi ini. Dalam hal ini, stempel notaris telah memberikan kontrak properti nonrepudiation, yang didefinisikan oleh NIAG sebagai kepastian pengirim data diberikan bukti pengiriman dan penerima diberikan bukti identitas pengirim, sehingga tidak dapat kemudian menyangkal telah memproses data.

Dalam dunia komunikasi digital, tidak ada notaris yang dapat mencap setiap pesan yang dikirimkan, tetapi nonrepudiation tetap diperlukan. Untuk memenuhi persyaratan ini, sistem yang aman biasanya mengandalkan kriptografi asimetris atau kunci publik. Sementara sistem kunci simetris menggunakan satu kunci untuk mengenkripsi dan mendekripsi data, sistem asimetris menggunakan pasangan kunci. Sistem ini menggunakan satu kunci pribadi untuk menandatangani data dan menggunakan kunci lainnya publik untuk memverifikasi data. Jika kunci yang sama dapat menandatangani dan memverifikasi konten pesan, pengirim dapat mengklaim bahwa siapa pun yang memiliki akses ke kunci tersebut dapat dengan mudah memalsukannya. Sistem kunci asimetris memiliki properti nonrepudiation karena penandatangan pesan dapat merahasiakan kunci pribadinya. Untuk informasi lebih lanjut tentang kriptografi asimetris, lihat artikel “State of the Hack” tentang subjek yang diterbitkan dalam Laporan Ancaman Mingguan edisi 6 Juli 2009.

2.1.1.4. Confidentiality

Istilah ini memiliki makna kerahasiaan dan secara umum istilah kerahasiaan sudah tidak asing lagi bagi kebanyakan orang, bahkan mereka yang tidak berkecimpung dalam industri keamanan. NIAG mendefinisikan makna kerahasiaan sebagai "jaminan bahwa informasi tidak diungkapkan kepada individu, proses, atau perangkat yang tidak berwenang atau berhak". Memastikan bahwa pihak yang tidak berwenang tidak memiliki akses ke sepotong informasi adalah tugas yang kompleks. Hal ini paling mudah untuk dipahami ketika dipecah menjadi tiga langkah utama. Pertama, informasi harus memiliki perlindungan yang mampu mencegah beberapa pengguna mengaksesnya. Kedua, batasan harus ada untuk membatasi akses ke informasi hanya bagi mereka yang memiliki otorisasi untuk melihatnya. Ketiga, sistem autentikasi harus ada untuk memverifikasi identitas mereka yang memiliki akses ke data. Autentikasi dan otorisasi, yang dijelaskan sebelumnya di bagian ini, sangat penting untuk menjaga kerahasiaan, tetapi konsep kerahasiaan terutama berfokus pada penyembunyian atau perlindungan informasi.

Salah satu cara untuk melindungi informasi adalah dengan menyimpannya di lokasi pribadi atau di jaringan pribadi yang dibatasi untuk mereka yang memiliki akses sah ke informasi tersebut. Jika suatu sistem harus mengirimkan data melalui jaringan publik, organisasi harus menggunakan kunci yang hanya diketahui oleh pihak yang berwenang untuk mengenkripsi data. Untuk informasi yang berjalan melalui Internet, perlindungan ini dapat berarti menggunakan *virtual private network* (VPN), yang mengenkripsi semua lalu lintas antara titik akhir, atau menggunakan sistem email terenkripsi, yang membatasi tampilan pesan ke penerima yang dituju. Jika informasi rahasia secara fisik meninggalkan lokasi yang dilindungi (seperti ketika karyawan membawa dan mengirimkan *hard disk* atau *flash disk*), maka organisasi harus mengenkripsi data jika jatuh ke tangan pengguna yang tidak berwenang maka akan membahayakan kerahasiaan dari informasi tersebut.

Kerahasiaan informasi digital juga membutuhkan kontrol di dunia nyata. Seperti contoh misalnya praktik melihat dari balik bahu seseorang saat berada di layar komputernya, adalah cara nonteknis bagi penyerang untuk mengumpulkan informasi rahasia. Ancaman fisik, seperti pencurian

sederhana, juga mengancam kerahasiaan, pencurian laptop atau *handphone*. Konsekuensi dari pelanggaran kerahasiaan bervariasi tergantung pada sensitivitas data yang dilindungi. Di Indonesia, pada awal 2000 banyak penggunaan kartu kredit secara ilegal untuk melakukan transaksi pembelian barang-barang luar negeri untuk masuk ke Indonesia. Hal ini disebabkan bocornya informasi kartu kredit sehingga dapat digunakan oleh khalayak dan sistem keamanan pada bank penerbit kartu kredit yang masih sangat lemah tanpa melibatkan autentikasi dan otorisasi.

2.1.1.5. Integrity

Kata ini mempunyai makna secara umum adalah asli, kesatuan, utuh atau terintegrasi. Di bidang keamanan informasi, integritas biasanya mengacu pada integritas data, atau memastikan bahwa data yang disimpan akurat dan tidak mengandung modifikasi yang tidak sah. National Information Assurance Glossary (NIAG) mendefinisikan integritas sebagai berikut yaitu kualitas SI (Sistem Informasi) yang mencerminkan kebenaran logis dan keandalan sistem operasi, kelengkapan logis dari perangkat keras dan perangkat lunak yang menerapkan mekanisme perlindungan; dan konsistensi struktur data dan kemunculan data yang disimpan. Perhatikan bahwa, dalam mode keamanan formal, integritas ditafsirkan lebih sempit sebagai perlindungan terhadap modifikasi atau penghancuran informasi yang tidak sah.

Aspek ini dapat dicapai dengan mempertimbangkan prinsip pada autentikasi, otorisasi, dan nonrepudiation sebagai kunci untuk menjaga integritas, mencegah mereka yang tidak memiliki otorisasi untuk memodifikasi data. Dengan melewati sistem autentikasi atau meningkatkan hak istimewa di luar yang biasanya diberikan kepada mereka, penyerang dapat mengancam integritas data dan dampaknya akan sangat merugikan.

Cacat dan kerentanan perangkat lunak dapat menyebabkan kerugian yang tidak disengaja dalam integritas data dan dapat membuka sistem untuk modifikasi yang tidak sah. Program biasanya mengontrol dengan ketat ketika pengguna memiliki akses baca-tulis ke data tertentu, tetapi kerentanan perangkat lunak memungkinkan untuk menghindari kontrol itu. Misalnya, penyerang dapat mengeksploitasi kerentanan Structured Query

Language (SQL) *injection* untuk mengekstrak, mengubah, atau menambahkan informasi ke *database*. Hal ini pernah terjadi dan menjadi kasus besar di Indonesia seperti mengubah data-data di KPU pada suatu pemilihan wakil rakyat di DPR.

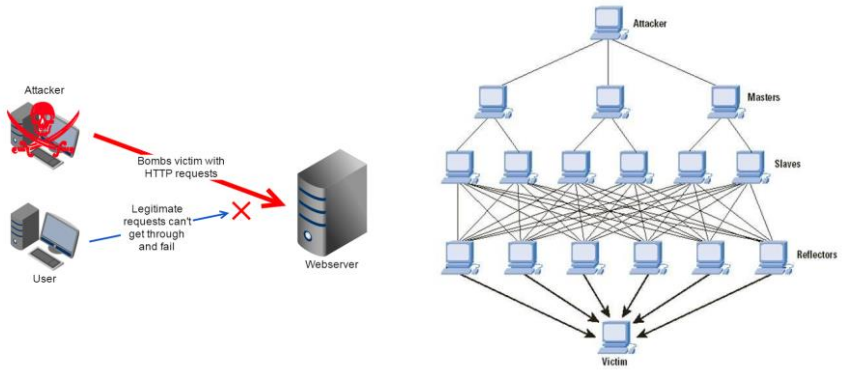
Mengganggu integritas data saat istirahat atau dalam pesan dalam perjalanan dapat memiliki konsekuensi yang sangat membahayakan. Jika memungkinkan untuk mengubah pesan transfer dana yang lewat antara pengguna dan situs web perbankan secara online, penyerang dapat menggunakan hak istimewa itu untuk mendapatkan keuntungan. Penyerang dapat mengambil alih nilai transfer dan mencuri dana yang ditransfer dengan mengubah nomor rekening penerima dana yang tercantum dalam pesan ke nomor rekening bank penyerang sendiri. Memastikan integritas jenis pesan ini sangat penting untuk sistem yang lebih aman.

2.1.1.6. Avalaibility

Terminologi ini mengacu para makna secara umum kepada makna ketersediaan. Sistem informasi harus dapat diakses oleh pengguna agar sistem ini memberikan nilai manffat kepada yang memerlukan. Jika sistem yang diperlukan tersebut mati atau dapat merespons namun terlalu lambat, sistem tidak dapat memberikan layanan yang seharusnya. NIAG mendefinisikan ketersediaan sebagai “akses tepat waktu dan andal ke layanan data dan informasi untuk pengguna yang berwenang.”

Serangan pada availability atau ketersediaan agak berbeda dari serangan pada integritas dan kerahasiaan. Serangan paling terkenal pada ketersediaan adalah *deniel of service* (DoS) atau jenis varian baru dari DoS yaitu DDoS (Distributed Deniel of Service). DoS dapat datang dalam berbagai bentuk, tetapi setiap bentuk mengganggu sistem dengan cara mencegah pengguna yang sah untuk mengaksesnya. Salah satu bentuk DoS adalah kelelahan sumber daya, di mana penyerang membebani sistem hingga tidak lagi merespons permintaan yang sah. Sumber daya yang dimaksud dapat berupa memori, waktu *central processing unit* (CPU), *bandwidth* jaringan, dan komponen lain apa pun yang dapat dipengaruhi oleh penyerang. Salah satu contoh serangan DoS adalah *network flooding*/banjir jaringan di mana penyerang mengirimkan begitu banyak

lalu lintas jaringan ke sistem yang ditargetkan sehingga lalu lintas memenuhi jaringan dan tidak ada permintaan yang sah yang dapat melewatinya.



A ilustrasi DoS B ilustrasi DDoS

Gambar 2.3 Perbedaan DoS dan DDoS

Memahami komponen triad CIA dan konsep di balik cara melindungi pelaku ini penting bagi setiap profesional keamanan. Setiap komponen bertindak seperti pilar yang menopang keamanan suatu sistem. Jika penyerang melanggar salah satu pilar, keamanan sistem akan jatuh. Autentikasi, otorisasi, dan nonrepudiation adalah alat yang dapat digunakan oleh perancang sistem untuk memelihara pilar-pilar ini. Memahami bagaimana semua konsep ini berinteraksi satu sama lain diperlukan untuk menggunakannya secara efektif agar tercipta sistem yang andal.

2.2. Kesimpulan

Para ahli sudah merumuskan bahwa untuk mencapai sistem keamanan yang ideal perlu tiga unsur penting yang harus diterapkan secara baik yaitu menyangkut aspek integritas, confidentiality dan availability. Ketiga aspek tersebut dirumuskan oleh lembaga yang sangat peduli dan konsen pada isu dan masalah *cyber security* yang dinamakan National Information Assurance Glossary (NIAG) yang diterbitkan Komite Sistem Keamanan

Nasional AS yang secara resmi dibentuk oleh pemerintahan Federal Amerika Serikat.

Autentikasi merupakan hal penting dalam mencapai sistem keamanan apa pun, karena itu adalah kunci untuk memverifikasi sumber pesan atau bahwa seseorang adalah siapa yang dia klaim. NIAG mendefinisikan autentikasi sebagai ukuran keamanan yang dirancang untuk menetapkan validitas transmisi, pesan, atau pencetus, atau sarana untuk memverifikasi otorisasi individu untuk menerima kategori informasi tertentu.

Istilah ini memiliki makna kerahasiaan dan secara umum istilah kerahasiaan sudah tidak asing lagi bagi kebanyakan orang, bahkan mereka yang tidak berkecimpung dalam industri keamanan. Kata ini juga mempunyai makna secara umum adalah asli, kesatuan, utuh atau terintegrasi. Di bidang keamanan informasi, integritas biasanya mengacu pada integritas data, atau memastikan bahwa data yang disimpan akurat dan tidak mengandung modifikasi yang tidak sah. Aspek ini dapat dicapai dengan mempertimbangkan prinsip pada autentikasi, otorisasi, dan nonrepudiation sebagai kunci untuk menjaga integritas, mencegah mereka yang tidak memiliki otorisasi untuk memodifikasi data.

Aspek berikutnya adalah *confidentiality* di mana salah satu cara untuk melindungi informasi adalah dengan menyimpannya di lokasi pribadi atau di jaringan pribadi yang dibatasi untuk mereka yang memiliki akses sah ke informasi tersebut. Jika suatu sistem harus mengirimkan data melalui jaringan publik, organisasi harus menggunakan kunci yang hanya diketahui oleh pihak yang berwenang untuk mengenkripsi data.

Aspek penting lainnya adalah availability yaitu ketersediaan. Terminologi ini mengacu para makna secara umum kepada makna ketersediaan. Sistem informasi harus dapat diakses oleh pengguna agar sistem ini memberikan nilai manfaat kepada yang memerlukan. Jika sistem yang diperlukan tersebut mati atau dapat merespons namun terlalu lambat, sistem tidak dapat memberikan layanan yang seharusnya. Serangan pada availability atau ketersediaan agak berbeda dari serangan pada integritas dan kerahasiaan. Serangan paling terkenal pada ketersediaan adalah *deniel of service* (DoS) atau jenis varian baru dari DoS yaitu DDoS (*Distributed Deniel of Service*).

2.3. Latihan

1. Apa yang membedakan serangan dalam bentuk DoS dan DDoS? Apakah kedua jenis serangan tersebut mempunyai dampak yang sama?
2. Bagaimana menangani atau mengantisipasi serangan dalam bentuk DoS atau DdoS tersebut?
3. Kedua serangan tersebut adalah masuk dalam aspek availability, Mengapa tidak masuk dalam kategori dampak yang lain?
4. Di akhir tahun 2022 ini masyarakat Indonesia dihebohkan munculnya pencurian data oleh salah satu hacker bernama Bjorka, mengapa hal tersebut bisa terjadi padahal sistem keamanan data pemerintah sudah dirancang seaman mungkin?
5. Bagaimana mengantisipasi serangan sejenis dengan pencurian data jika mungkin muncul di masa yang akan datang?

BAB III

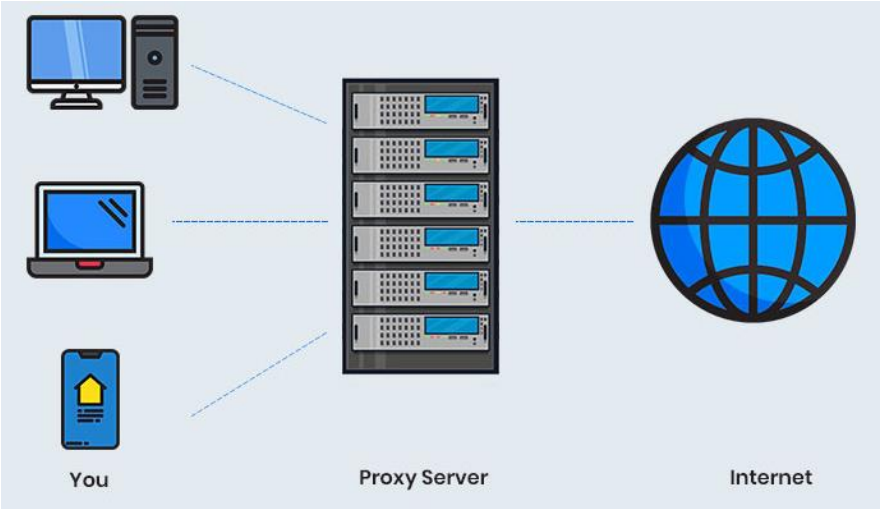
TEKNIK DAN MOTIVASI MENYERANG

3.1. Pendahuluan

3.1.1. Penggunaan *Proxy*

Menutupi alamat IP seseorang adalah praktik standar saat melakukan aktivitas terlarang. Proksi yang dikonfigurasi dengan baik memberikan anonimitas yang kuat dan tidak mencatat aktivitas, sehingga membuat upaya penegakan hukum gagal untuk mengidentifikasi lokasi asli orang yang terlibat.

Sebuah *proxy* memungkinkan aktor untuk mengirim lalu lintas jaringan melalui komputer lain, yang memenuhi permintaan dan mengembalikan hasilnya. Siswa atau karyawan dapat menggunakan *proxy* untuk berkomunikasi dengan layanan yang diblokir seperti Internet Relay Chat (IRC) dan pesan instan, atau untuk menelusuri situs web yang diblokir oleh administrator. Penyerang juga menggunakan *proxy* karena alamat Internet Protocol (IP) dapat dilacak, dan mereka tidak ingin mengungkapkan lokasi mereka yang sebenarnya. Sebagai salah satu contoh, iDefense menulis tentang arsitektur aliran cepat (ID# 484463), yang menggunakan infrastruktur *proxy* untuk memenuhi permintaan. Proksi juga merupakan sumber umum pesan email spam, yang menggunakan relai terbuka *simple mail* transport *protocol* (SMTP). Contoh dari skema *proxy* dalam koneksi internet pada Gambar 3.1.



Gambar 3.1 Skema *proxy* dalam membangun koneski internet

Proxy berguna bagi penyerang dalam banyak hal. Kebanyakan penyerang menggunakan *proxy* untuk menyembunyikan alamat IP mereka dan, oleh karena itu, lokasi fisik mereka yang sebenarnya. Dengan cara ini, penyerang dapat melakukan transaksi keuangan palsu, melancarkan serangan, atau melakukan tindakan lain dengan risiko kecil. Sementara penegak hukum dapat mengunjungi lokasi fisik yang diidentifikasi oleh alamat IP, penyerang yang menggunakan satu atau beberapa *proxy* melintasi batas negara lebih sulit ditemukan. Titik akhir hanya dapat melihat *proxy* terakhir yang berkomunikasi langsung dengannya dan bukan *proxy* perantara atau lokasi aslinya.

Proksi menyediakan cara bagi penyerang untuk menurunkan risiko mereka dalam identifikasi penyelidik atas alamat IP mereka yang sebenarnya. Dalam serangan hipotetis, file log korban hanya berisi satu dari banyak alamat IP yang dibutuhkan penyidik untuk menemukan penyerang. Penyerang mengoperasikan *proxy* gratis atau mengubah pengaturan *proxy* korban karena *proxy* dapat berfungsi sebagai alat pemantauan. Anon*Proxy* adalah salah satu contoh *proxy* jahat yang dirancang oleh pembuatnya untuk memantau pengguna dan mencuri informasi seperti kata sandi jaringan sosial karena *proxy* menyampaikan lalu lintas maka ia juga memiliki kemampuan untuk mencatat dan

mengubah halaman atau informasi sensitif. Penyerang harus meyakinkan pengguna atau menginstal kode berbahaya untuk mengubah pengaturan *proxy* sendiri.

Pembuat kode berbahaya juga menginstal *proxy* lokal dengan mengubah file host atau konfigurasi browser untuk menggunakan *proxy*, penyerang mengarahkan permintaan dan menangkap informasi rahasia. Beberapa Trojan untuk menyerang perusahaan perbankan memberi penyerang kemampuan untuk meminta *proxy* melalui browser korban karena melakukan penipuan dari alamat IP pengguna yang sah kurang mencurigakan. *Proxy* lokal lebih sulit untuk diidentifikasi karena *proxy* lokal tidak membuka *port* jaringan apa pun dan pemindaian sistem tidak akan mengungkapkan perubahan apa pun.

3.1.1.1. Jenis *Proxy*

Proxy sangat umum digunakan oleh user sehingga banyak penyerang melakukan *scanning* pada internet untuk mendengarkan *port proxy* yang umum. *Proxy* yang paling umum mendengarkan pada *port* TCP 80, 8000, 8081, 443, 1080 (SOCKS *Proxy*), dan 3128 yang digunakan Squid *Proxy*, dan beberapa juga menangani User Datagram Protocol (UDP). Penyerang yang memasang *proxy* khusus sering kali tidak menggunakan *port* standar tetapi menggunakan *port* tinggi yang acak. Beberapa *proxy* ringan ditulis dalam bahasa script yang dijalankan dengan server HTTP dan lebih mudah dimodifikasi oleh penyerang. Aplikasi *proxy* memerlukan konfigurasi. Beberapa aplikasi tidak beroperasi dengan benar melalui layanan *proxy* karena server *proxy* menghapus informasi yang diperlukan atau tidak dapat memenuhi permintaan. Beberapa layanan seperti The Onion Router (TOR2) juga memberi pengguna kemampuan untuk mem-*proxy* lalu lintas dan menyembunyikan lokasi asli mereka dari korban.

Aplikasi VPN dapat bertindak sebagai *proxy* yang lebih fleksibel dan mendukung lebih banyak fitur keamanan. Alih-alih mengonfigurasi aplikasi untuk menggunakan *proxy*, pengguna dapat melakukan tunnel semua lalu lintas melalui VPN. Layanan VPN biasanya mendukung autentikasi yang *secure* dan cenderung tidak membocorkan informasi yang dapat mengidentifikasi pengguna *proxy*.