HACKER VS DEFENDER

Panduan Komprehensif dari Serangan hingga Pertahanan Siber

Tim Penulis:

Dedy Iskandar
Agung Yuliyanto Nugroho
Nasril Sany
Haryanto
Rosmawati Dwi
Martono
Lilis Supratman
Abdul Wahid

HACKER VS DEFENDER

Panduan Komprehensif dari Serangan hingga Pertahanan Siber

Dedy Iskandar
Agung Yuliyanto Nugroho
Nasril Sany
Haryanto
Rosmawati Dwi
Martono
Lilis Supratman
Abdul Wahid

sada
kurnia pustaka

HACKER VS DEFENDER

Panduan Komprehensif dari Serangan hingga Pertahanan Siber

Tim Penulis:
Dedy Iskandar
Agung Yuliyanto Nugroho
Nasril Sany
Haryanto
Rosmawati Dwi
Martono
Lilis Supratman
Abdul Wahid

Editor : Ajay Supriadi, M.Kom.
Tata Letak : Lilis Khalisatul Karimah, S.H.
Desain Cover : Septimike Yourintan Mutiara, S.Gz.
Ukuran : UNESCO 15,5 x 23 cm
Halaman : vii, 180
ISBN : 978-634-7522-03-0
Terbit Pada : Desember 2025
Anggota IKAPI : No. 073/BANTEN/2023

PENERBIT PT SADA KURNIA PUSTAKA
Jl. Warung Selikur Km.6 Sukajaya – Carenang, Kab. Serang-Banten
Email : sadapenerbit@gmail.com
Website : sadapenerbit.com & repository.sadapenerbit.com
Telpon/WA : +62 838 1281 8431

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya, sehingga buku berjudul ***HACKER VS DEFENDER: Panduan Komprehensif dari Serangan hingga Pertahanan Siber*** ini dapat diselesaikan.

Dalam era digital yang terus melesat, dunia siber telah menjadi medan pertempuran baru yang tak kasat mata. Di satu sisi, ancaman siber terus berevolusi dengan kecepatan yang mengkhawatirkan, mulai dari eksploitasi sederhana hingga serangan canggih yang didanai negara. Di sisi lain, para profesional keamanan siber dituntut untuk selalu sigap, waspada, dan terus belajar untuk membangun pertahanan yang tangguh. Buku ini hadir untuk menjembatani kedua dunia tersebut, membahas taktik, teknik, dan prosedur dari kedua perspektif baik dari sudut pandang penyerang (*hacker*) maupun pembela (*defender*).

Tujuan utama penulisan buku ini bukan untuk mengajarkan kejahatan, melainkan untuk memberikan pemahaman yang mendalam dan holistik. Dengan memahami bagaimana sebuah serangan dilancarkan, kita akan mampu merancang dan mengimplementasikan strategi pertahanan yang jauh lebih efektif dan proaktif. *"Untuk mengalahkan musuh, Anda harus mengenal musuh Anda."* Prinsip inilah yang menjadi fondasi setiap bab dalam buku ini.

Buku ini dirancang secara komprehensif, mulai dari konsep dasar keamanan siber, tahapan peretasan (*ethical hacking*) yang terstruktur, analisis berbagai vektor serangan (seperti *malware, phishing, SQL Injection*, hingga *Advanced Persistent Threat*), hingga langkah-langkah praktis untuk membangun dan mengoperasikan *Security Operations Center (SOC)*, melakukan *incident response*, dan membentuk budaya keamanan dalam organisasi. Materi disajikan dengan bahasa yang jelas, studi kasus nyata, dan panduan praktis yang dapat diterapkan, baik untuk akademisi, profesional IT, mahasiswa, maupun siapapun yang tertarik mendalami dunia keamanan digital.

Akhir kata, semoga setiap halaman dalam buku ini membawa pencerahan dan kontribusi positif bagi penguatan ekosistem keamanan siber di Indonesia. Selamat membaca, dan mari bersama-sama membangun pertahanan siber yang lebih tangguh.

Tim Penulis

DAFTAR ISI

BAB 1
DUNIA *HACKER* DAN *DEFENDER*

Dedy Iskandar, S.Kom., M.T.I.
Universitas Raharja Tangerang

Pendahuluan

Dunia *cyber security* merupakan arena dinamis yang mempertemukan dua kubu dengan kepentingan berlawanan: *hacker* dan *defender*. Hacker adalah individu atau kelompok yang memiliki kemampuan teknis untuk mengeksplorasi, memodifikasi, atau menembus sistem komputer, baik dengan tujuan positif (*ethical*) maupun negatif (*malicious*).

Sementara itu, *defender* adalah pihak yang bertugas menjaga, melindungi, serta mengamankan sistem dari berbagai ancaman *digital*. Seiring berkembangnya teknologi, taktik serangan para *hacker* semakin kompleks, memaksa para *defender* untuk terus meningkatkan kemampuan dan strategi pertahanan.

Dalam konteks etika, tidak semua *hacker* adalah kriminal. Terdapat tiga kategori utama: *white hat,* yaitu *hacker* etis yang membantu mendeteksi kerentanan; *black hat*, yaitu penyerang yang menembus sistem untuk keuntungan pribadi; dan *grey hat*, yang berada di antara keduanya. Perkembangan ini menunjukkan bahwa hacker bukan sekadar pelaku kejahatan, tetapi juga aktor penting dalam memperkuat keamanan *digital*.

Di sisi lain, dunia *defender* dituntut memahami pola pikir *hacker* untuk dapat membangun pertahanan yang adaptif, responsif, dan berlapis. Serangan siber modern seperti *phishing*, *malware*, *ransomware*, hingga *zero-day exploit* menuntut keamanan TI untuk menerapkan strategi pertahanan yang komprehensif. Pendekatan seperti *defense-in-depth*, *threat intelligence*, *incident response*, serta penggunaan teknologi seperti SIEM dan AI menjadi senjata utama para *defender*. Hubungan antara *hacker* dan *defender* sesungguhnya merupakan siklus evolutif: setiap serangan baru melahirkan mekanisme pertahanan baru, dan setiap pertahanan baru mendorong munculnya teknik serangan yang lebih canggih.

Sebagaimana dikemukakan oleh Bruce Schneier, salah satu pakar keamanan informasi dunia, *"Security is a process, not a product"*. Kutipan ini menegaskan bahwa keamanan tidak pernah berhenti pada satu titik, melainkan merupakan proses berkelanjutan yang harus terus diperbarui seiring berkembangnya ancaman.

kubu *defender*, yaitu tindakan cepat yang dilakukan oleh seorang analis keamanan bernama Marcus Hutchins, yang berhasil menemukan *kill switch* yang menghentikan penyebaran *ransomware* tersebut.

Kasus ini menunjukkan bagaimana serangan hacker dapat menimbulkan kerusakan besar dalam waktu singkat, sementara peran defender sangat penting untuk menghentikan serangan, memulihkan sistem, dan mencegah kerusakan lebih lanjut. Contoh lainnya adalah serangan DDoS terhadap Dyn pada tahun 2016, yang membuat layanan besar seperti *Twitter, Netflix*, dan *Spotify* tidak dapat diakses; dalam kasus ini, para *defender* dari berbagai perusahaan keamanan bekerja sama memblokir sumber serangan dan memulihkan stabilitas jaringan.

Melalui contoh-contoh tersebut, terlihat jelas bahwa konflik antara *hacker* dan *defender* merupakan dinamika yang terus berkembang di dunia siber.

Tantangan dan Hambatan *Hacker* dan *Defender*

Baik *hacker* maupun defender menghadapi berbagai tantangan dan hambatan dalam menjalankan aktivitas mereka di dunia siber yang terus berkembang. Di sisi *hacker*, tantangan utama adalah peningkatan teknologi keamanan yang semakin kuat, seperti enkripsi tingkat tinggi, sistem deteksi intrusi, dan pembaruan keamanan yang cepat, sehingga mereka harus terus mempelajari teknik baru untuk menemukan celah.

Selain itu, *hacker* juga menghadapi risiko hukum, karena sebagian besar aktivitas mereka melanggar undang-undang dan dapat menyebabkan hukuman berat. Hambatan lain bagi *hacker* adalah keterbatasan informasi tentang target serta kebutuhan akan kemampuan teknis yang terus meningkat. Di sisi lain, defender menghadapi tantangan yang tidak kalah kompleks, termasuk evolusi serangan yang semakin canggih**,** seperti *ransomware*, serangan *zero-day,* dan serangan berbasis AI yang sulit dideteksi.

Defender juga harus menangani keterbatasan sumber daya, seperti kurangnya tenaga ahli keamanan, anggaran yang minim, dan infrastruktur lama yang rentan. Selain itu, mereka harus mengatasi

faktor manusia, karena kelalaian pengguna sering menjadi pintu masuk utama serangan. Tantangan terbesar *defender* adalah mempertahankan keamanan secara konsisten 24/7, sementara hacker hanya membutuhkan satu celah kecil untuk berhasil. Perbedaan tantangan ini menunjukkan betapa kompleksnya dinamika pertahanan dan serangan dalam ekosistem keamanan siber modern.

Tren Masa Depan Dunia *Hacker* dan *Defender*

Tren masa depan dunia *hacker* dan *defender* diprediksi akan semakin kompleks seiring berkembangnya teknologi *digital*. Di sisi *hacker*, serangan diperkirakan memanfaatkan kecerdasan buatan (AI) dan *machine learning***,** memungkinkan otomatisasi eksploitasi, pencarian celah keamanan, hingga serangan yang lebih sulit dideteksi.

Hacker juga akan semakin banyak menargetkan perangkat IoT, kendaraan otonom, dan infrastruktur kritis yang terhubung, karena keamanan perangkat ini sering lebih lemah. Selain itu, teknik serangan berbasis *deepfake* dan rekayasa sosial tingkat lanjut diperkirakan menjadi ancaman yang semakin besar karena sulit dibedakan dengan aktivitas manusia. Sementara itu, *defender* dimasa depan akan mengandalkan AI berbasis deteksi perilaku, keamanan prediktif, dan *threat intelligence* global yang dapat mengenali ancaman sebelum terjadi. Teknologi seperti *zero trust architecture*, autentikasi biometrik, dan enkripsi kuantum juga akan menjadi standar dalam pertahanan.

Namun, *defender* tetap akan menghadapi tantangan besar berupa kekurangan tenaga ahli keamanan, serangan yang beradaptasi cepat, serta meningkatnya kerumitan sistem *digital*. Tren ini menunjukkan bahwa masa depan keamanan siber adalah perang kecerdasan antara algoritma penyerang dan algoritma pembela, dimana inovasi berkelanjutan menjadi satu-satunya jalan untuk bertahan.

Revolusi *Hacker*

Revolusi *hacker* telah mentransformasi *landscape* teknologi dan keamanan *digital* secara fundamental, berevolusi dari sekelompok kecil *enthusiasts* yang terpinggirkan menjadi kekuatan global yang mempengaruhi kebijakan keamanan nasional, inovasi teknologi, dan ekonomi *digital*.

Dimulai dari komunitas mahasiswa MIT pada 1960-an yang mempelopori eksplorasi sistem komputer *mainframe*, revolusi ini melalui tiga fase transformatif yang signifikan. Fase pertama (1980-1990) ditandai dengan munculnya "*phone phreaks*" dan *Bulletin Board Systems* (BBS) yang membentuk jaringan kolaborasi awal, meski sering dikriminalisasi oleh otoritas.

Fase kedua (1990-2000) menyaksikan profesionalisasi dengan lahirnya *ethical hacking* sebagai disiplin formal, diikuti pengakuan industri terhadap bug *bounty programs* sebagai mekanisme keamanan yang *legitimate*. Fase ketiga (2000-sekarang) menandai *era state-sponsored hacking* dimana kemampuan teknis *hacker* menjadi alat geopolitik yang *powerful*, sementara *simultaneously* memunculkan gerakan *hacktivism* yang memanfaatkan keahlian *digital* untuk tujuan politik dan sosial.

Revolusi ini tidak hanya menghasilkan inovasi teknis seperti *open-source software* dan metode enkripsi, tetapi juga menciptakan ekosistem ekonomi baru bernilai miliaran dolar melalui *cybersecurity industry*, sambil terus menantang batasan-batasan regulasi dan etika di era *digital*.

Revolusi *Defender*

Revolusi *defender* dalam dunia keamanan siber berlangsung seiring meningkatnya kompleksitas ancaman *digital* dan berkembangnya teknologi modern. Pada awalnya, defender hanya mengandalkan keamanan dasar seperti antivirus dan *firewall* statis, namun kini pendekatan tersebut tidak lagi cukup menghadapi serangan yang semakin canggih.

Dalam revolusi pertahanan siber modern, defender beralih ke sistem keamanan berbasis kecerdasan buatan, *machine learning*, serta *behavioral analytics* yang mampu mendeteksi pola anomali secara *real-time.* Selain itu, konsep *Zero Trust Architecture* menjadi revolusi besar karena tidak lagi mengandalkan kepercayaan bawaan, melainkan memverifikasi setiap akses secara ketat.

Di tingkat organisasi, defender kini lebih proaktif melalui threat hunting, *continuous monitoring*, dan integrasi *Security Operation*

Center (SOC) berbasis otomatisasi. Perkembangan teknologi seperti SIEM generasi baru, SOAR, enkripsi kuantum, dan keamanan *cloud-native* telah mengubah peran *defender* dari sekadar pengawas menjadi arsitek pertahanan yang adaptif, analitis, dan responsif. Revolusi ini menegaskan bahwa pertahanan modern tidak lagi reaktif, tetapi prediktif dan dinamis**,** menyesuaikan diri dengan ancaman yang terus berkembang.

Daftar Pustaka

Anderson, Ross. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.

Andress, J. & Winterfeld, S. (2014). *Cyber Warfare: Techniques, Tactics And Tools for Security Practitioners (2nd ed.).* Syngress.

Coleman, E. G. (2013). *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton University Press.

EC-Council. (2021). *Certified Ethical Hacker (CEH) Official Study Guide.* EC-Council Press.

Erickson, J. (2008). *Hacking: The Art of Exploitation (2nd ed.).* No Starch Press. Wikipedia.

Erickson, Jon. (2008). *Hacking: The Art of Exploitation*. No Starch Press.

Greenberg, A. (2012). *This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information*. Dutton.

Levy, S. (2010). *Hackers: Heroes of The Computer Revolution (25th Anniversary Edition).* O'Reilly Media.

Mitnick, Kevin. (2003). *The Art of Deception: Controlling the Human Element of Security.* Wiley.

MITRE Corporation. (n.d.). *MITRE ATT&CK® Knowledge Base.* https://attack.mitre.org/.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST. (see: NIST CSF 2.0). NIST Publications.

NIST. (2020). *NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations*. NIST Publications.

OWASP Foundation. (2021). *OWASP Top Ten 2021: The Ten Most Critical Web Application Security Risks.* https://owasp.org/www-project-top-ten/.

Sanger, D. E. (2018). *The Perfect Weapon: War, Sabotage, and Fear in The Cyber Age*. Crown Publishing Group.

Schneier, Bruce. (2000). *Secrets And Lies: Digital Security In A Networked World.* Wiley,

Sikorski, M., & Honig, A. (2012). *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press. nostarch.com.

Stallings, William. (2017). *Network Security Essentials: Applications And Standards.* Pearson.

Stuttard, D., & Pinto, M. (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws* (2nd ed.). Wiley. O'Reilly Media.

Thomas, D. (2002). *Hacker Culture*. University of Minnesota Press.

PROFIL PENULIS

Dedy Iskandar, S.Kom., M.T.I.

Penulis Lulus S1 Program Studi Sistem Informasi di Sekolah Tinggi Manajemen dan Ilmu Komputer (STMIK) Bina Darma Palembang dan menyelesaikan Program Studi Magister Teknik Informatika Sekolah Tinggi Manajemen dan Ilmu Komputer (STMIK) Raharja Tangerang. Saat ini sebagai Dosen Fakultas Sains dan Teknologi Universitas Raharja. Saya juga masih mengajar di SMK Pustek Serpong, dan juga sebagai Tutor *Online* pada Universitas Terbuka. Penulis mengampu mata kuliah Rekayasa Sistem, Logika Algoritma dan Pemrograman, Sistem Basis Data, Organisasi Komputer, Jaringan Komputer, Struktur Data. Aktif sebagai penulis di beberapa Jurnal nasional yang terindeks Sinta 3 dan Sinta 4. Sekarang saya juga aktif di beberapa organisasi seperti Partai Golkar sebagai Ketua Ranting dan Kosgoro sebagai Ketua Pelatihan dan Pengembangan.

Email Penulis: iskandar@raharja.info.

BAB 2
KONSEP DASAR IT
SECURITY

Agung Yuliyanto Nugroho, M.Kom., M.Par.
Universitas Cendekia Mitra Indonesia

Apa Itu IT *Security*?

Dalam era *digital*, informasi telah menjadi sumber daya paling berharga setelah energi. Data bukan sekadar catatan angka atau teks, melainkan cerminan aktivitas sosial, ekonomi, politik, hingga identitas manusia. Setiap klik, transaksi, dan interaksi daring meninggalkan jejak yang dapat dimanfaatkan baik untuk kemajuan, maupun untuk kejahatan.

Fenomena inilah yang melahirkan satu bidang ilmu penting bernama Keamanan Teknologi Informasi (*Information Technology Security*), atau lebih sering disingkat IT *Security*. Disiplin ini bertujuan utama untuk melindungi sistem, jaringan, dan data dari akses, perubahan, atau kerusakan yang tidak sah. Pada masa komputer generasi pertama, fokus utama pengembang bukan pada keamanan, melainkan pada fungsionalitas.

Komputer seperti ENIAC dan UNIVAC digunakan untuk perhitungan ilmiah dan militer. Hanya segelintir orang yang memiliki akses, sehingga ancaman keamanan masih terbatas pada kesalahan manusia atau kerusakan mesin. Namun, saat komputer mulai digunakan bersama (*time-sharing systems*), muncullah kebutuhan untuk mengatur akses pengguna.

Tahun 1960-an, MIT mengembangkan *Compatible Time-Sharing System* (CTSS), yang memperkenalkan konsep *password* langkah pertama dalam sejarah keamanan komputer modern. Akan tetapi, pada 1965 seorang mahasiswa bernama Allan Scherr berhasil mencuri *file password* CTSS untuk membuktikan bahwa sistem tersebut dapat ditembus. Peristiwa ini sering disebut sebagai salah satu insiden keamanan komputer pertama ketika ARPANET, cikal bakal Internet, dibangun pada akhir 1960-an, para penelitinya tidak membayangkan bahwa jaringan tersebut suatu hari akan menjadi arena serangan global.

Desain awal ARPANET berlandaskan kepercayaan semua pengguna dianggap sah dan bertanggung jawab. Namun pada tahun 1988, dunia dikejutkan oleh The Morris Worm, serangan pertama yang menyebar luas melalui Internet. Worm ini menyebabkan kerugian besar dan menandai lahirnya disiplin baru yang dikenal sebagai *Cybersecurity*. Pemerintah Amerika Serikat kemudian membentuk lembaga khusus seperti *Computer Emergency Response Team* (CERT) untuk menangani ancaman siber.di dunia.

Perkembangan pesat Internet, media sosial, dan perangkat *mobile* mengubah lanskap ancaman. Serangan tidak lagi hanya datang dari peretas individu, tetapi juga kelompok terorganisir, sindikat kejahatan siber, bahkan aktor negara. Serangan *ransomware*, kebocoran data pribadi, dan sabotase infrastruktur kritis menjadi tantangan baru. Di sisi lain, muncul pula profesi *ethical hacker*, *security analyst*, dan *digital forensic investigator* menunjukkan bahwa keamanan kini bukan sekadar aspek teknis, tetapi fondasi kepercayaan dalam ekosistem *digital*.

Secara konseptual, IT Security adalah serangkaian proses, kebijakan, dan teknologi yang dirancang untuk melindungi sistem informasi dari ancaman yang dapat mengganggu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data serta layanan *digital*. Definisi ini dikenal luas sebagai model CIA triad, yang menjadi prinsip dasar keamanan informasi:

1. ***Confidentiality* (Kerahasiaan)**
   Memastikan bahwa hanya pihak yang berwenang yang dapat mengakses data. Contohnya: penggunaan enkripsi pada komunikasi *email* untuk mencegah penyadapan.
2. ***Integrity* (Integritas)**
   Menjamin bahwa data tidak dapat diubah tanpa izin atau terdeteksi bila terjadi perubahan. Misalnya: tanda tangan *digital* pada dokumen elektronik.
3. ***Availability* (Ketersediaan)**
   Memastikan bahwa sistem dan data selalu dapat diakses saat dibutuhkan. Misalnya: *server* cadangan (*backup server*) untuk menjaga layanan tetap aktif saat terjadi serangan DDoS.

Selain CIA, banyak pakar menambahkan prinsip lain seperti *authentication* (autentikasi), *authorization* (otorisasi), dan *accountability* (pertanggungjawaban), yang membentuk kerangka keamanan komprehensif dalam sistem informasi modern. IT *Security* bukan hanya tentang memasang antivirus atau *firewall*, melainkan mencakup strategi menyeluruh yang mencakup empat lapisan utama:

1. Keamanan Fisik: melindungi perangkat keras dan infrastruktur (ruang *server*, kabel, UPS).
2. Keamanan Jaringan: mengamankan lalu lintas data melalui *firewall*, IDS/IPS, dan enkripsi.

atau kompromi kredensial. Setelah penyerang berhasil masuk, mereka sering melakukan pergerakan lateral di jaringan, mencari aset bernilai, meningkatkan hak akses untuk memperoleh kontrol lebih luas, memasang mekanisme persistensi agar kehadiran mereka sulit dihapus, dan akhirnya menyiapkan saluran C2 untuk menerima perintah serta mengekstrak data atau menghancurkan operasi.

Model serangan juga menekankan bahwa operasi penyerang bersifat adaptif dan berlapis; teknik yang efektif dalam satu lingkungan belum tentu berhasil di lingkungan lain, sehingga pelaku sering melakukan *reconnaissance* berulang dan menyesuaikan taktik sesuai arsitektur target. Contoh realistik: sebuah kelompok kriminalisasi siber mungkin memulai dengan kampanye *spear-phishing* untuk menggaet kredensial pegawai tingkat menengah, lalu memanfaatkan kredensial tersebut untuk mengakses *server file,* menjalankan *credential dumping* untuk mendapatkan akun domain admin, lalu memindahkan *ransomware* ke *server* produksi untuk mengenkripsi data. Setiap tahap memberi peluang bagi *defender* untuk mendeteksi (*log* anomali *login*), memutus (menonaktifkan akun yang terindikasi), atau merespons (*isolate endpoint*).

Untuk merancang pertahanan yang efektif, model serangan mengarahkan *defender* pada tiga prinsip praktis. Pertama, deteksi dini menempatkan sensor pada titik yang sering dilalui penyerang (*perimeter email, gateway web, endpoint*, dan *log* autentikasi) untuk mengenali aktivitas pengintaian, *credential abuse*, atau eksekusi kode berbahaya. Kedua, gangguan/mitigasi berlapis menerapkan kontrol preventif (MFA, *patching, segmentation*), kontrol detektif (EDR, IDS/IPS, SIEM), dan kontrol responsif (*playbook* IR, isolasi jaringan, *backup*) sehingga kegagalan satu lapis tidak mengakibatkan kompromi total.

Ketiga, pemodelan ancaman dan *hunting* menggunakan intelijen ancaman dan peta teknik (seperti ATT&CK) untuk melakukan threat hunting proaktif terhadap teknik yang paling mungkin digunakan oleh aktor yang relevan dengan organisasi. Model serangan juga berguna untuk komunikasi antar pemangku kepentingan. Dengan memetakan insiden ke tahap-tahap model, tim keamanan dapat menjelaskan kepada manajemen bagaimana sebuah pelanggaran terjadi, mengapa

kontrol tertentu gagal, dan mengapa investasi pada area-area spesifik (misalnya EDR atau segmentasi jaringan) akan menurunkan risiko pada tahap-tahap kritikal.

Selain itu, pemahaman model memfasilitasi latihan *red team*/*blue team* yang realistis: *red team* mensimulasikan rangkaian taktik untuk menguji kemampuan deteksi dan respons, sementara blue team menguji kemampuan mereka memutuskan serangan di berbagai tahap *Kill Chain* atau mengidentifikasi teknik ATT&CK yang dipakai. Beberapa contoh singkat yang mengilustrasikan aplikasi model serangan memperjelas nilai praktisnya. Dalam serangan *supply-chain*, pelaku memodifikasi pembaruan perangkat lunak *vendor* sehingga *payload* berbahaya terdistribusi keratusan organisasi. Model serangan menunjukkan bagaimana fokus harus diletakkan pada verifikasi integritas *update* (*code signing*), deteksi perilaku abnormal setelah *patch* berjalan, serta segmentasi untuk membatasi dampak.

Dalam serangan yang berawal dari IoT yang tidak ter*patch* di jaringan kantor, model menggarisbawahi pentingnya *inventory* perangkat, kebijakan *network access control* untuk IoT, dan monitoring perilaku jaringan untuk mendeteksi *lateral movement* dari perangkat *non-trusted.* Akhirnya, meskipun model serangan seperti *Kill Chain* dan ATT&CK memberikan peta yang sangat berguna, *defender* sebaiknya menganggap model tersebut bukan sebagai resep kaku, tetapi sebagai lensa untuk memahami pola. Dunia nyata penuh ketidakpastian: pelaku berubah, teknik baru muncul, dan konteks organisasi berbeda-beda.

Oleh karena itu, implementasi yang tangguh menggabungkan pemahaman model dengan praktik adaptif: pembaruan intelijen ancaman, otomasi respons, latihan berkala, dan kolaborasi lintas tim serta dengan komunitas keamanan yang lebih luas. Dengan demikian, memahami model serangan bukan tujuan akhir; ia adalah langkah awal untuk membangun sistem yang mampu mendeteksi, menahan, dan pulih dari serangan dalam ekosistem *digital* yang terus berubah.

Daftar Pustaka

Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.).* Wiley.

Casey, E. (2019). *Digital Evidence And Computer Crime: Forensic Science, Computers, And The Internet (4th ed.).* Academic Press.

Cole, E., Krutz, R. L., & Conley, J. (2019). *Network Security Bible (3rd ed.).* Wiley.

Harris, S. (2022). *CISSP All-In-One Exam Guide (9th ed.).* McGraw-Hill Education.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed By Analysis of Adversary Campaigns And Intrusion Kill Chains. *Leading Issues in Information Warfare & Security Research*, 1(1), 80–106.

Kim, D., & Solomon, M. G. (2020). *Fundamentals of Information Systems Security* (3rd ed.). Jones & Bartlett Learning.

MITRE. (2023). *ATT&CK®: Adversarial Tactics, Techniques, And Common Knowledge*. MITRE Corporation. https://attack.mitre.org

Pfleeger, C. P., & Pfleeger, S. L. (2021). *Security In Computing (6th ed.).* Pearson.

Von Solms, R., & Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004.

Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security (6th ed.).* Cengage Learning.

PROFIL PENULIS

Agung Yuliyanto Nugroho, M.Kom., M.Par.

Ketertarikan penulis terhadap ilmu komputer dimulai pada tahun 2015 silam. Hal tersebut membuat penulis melanjutkan pendidikan ke Perguruan Tinggi dan berhasil menyelesaikan studi S1 di prodi Teknik Informatika Universitas Teknologi Yogyakarta pada tahun 2018. Dua tahun kemudian, penulis menyelesaikan studi S2 di prodi Teknik Informatika Program Pasca Sarjana Universitas Amikom Yogyakarta dan juga prodi Magister Pariwisata di Sekolah Tinggi Pariwisata Ambarrukmo Yogyakarta. Atas dedikasi dan kerja keras dalam membuat suatu karya, Republik Indonesia Kementerian Hukum dan Hak Asasi Manusia sudah mencatat ada kurang lebih 100 karya yang sudah tercatat di surat pencatatan ciptaan sebagai salah satu kontribusi dalam melindungi hak kekayaan intelektual.

Email Penulis: agungboiler11@gmail.com.

BAB 3
JENIS-JENIS ANCAMAN SIBER

Nasril Sany, S.Kom., M.Kom.
Institut Teknologi PLN

Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar terhadap berbagai aspek kehidupan manusia, termasuk cara berinteraksi, bertransaksi, dan mengelola data. Namun, kemajuan digital ini juga diiringi dengan meningkatnya ancaman terhadap keamanan informasi atau yang dikenal sebagai ancaman siber (*cyber threats*). Ancaman siber merupakan segala bentuk upaya yang bertujuan untuk mengganggu, merusak, mencuri, atau mengakses informasi dan sistem komputer tanpa izin (IBM, n.d.).

Menurut Suharto (2021), ancaman siber adalah tindakan yang memanfaatkan kerentanan sistem komputer dan jaringan dengan maksud merugikan pihak lain, baik individu, organisasi, maupun negara. Bentuk ancaman ini dapat berupa serangan *malware,* pencurian identitas, peretasan jaringan, hingga spionase *digital*. Dampak dari serangan tersebut tidak hanya bersifat teknis, tetapi juga dapat menimbulkan kerugian ekonomi, sosial, dan reputasi.

Pakar keamanan siber Kevin Mitnick menyatakan bahwa "*The weakest link in the security chain is the human element*" elemen manusia merupakan mata rantai terlemah dalam sistem keamanan (Orsys, 2025). Pernyataan ini menegaskan bahwa kesadaran dan perilaku pengguna juga berperan besar dalam terjadinya ancaman siber. Selain faktor manusia, Mikko Hyppönen, seorang ahli keamanan dari *F-Secure*, menambahkan bahwa "*If it's smart, it's vulnerable*" artinya setiap perangkat pintar (*smart device*) yang terhubung ke internet memiliki potensi untuk diserang (Hyppönen, 2023). Berbagai penelitian menunjukkan bahwa frekuensi dan kompleksitas serangan siber terus meningkat seiring dengan kemajuan teknologi, seperti *Internet of Things* (IoT), kecerdasan buatan (AI), dan komputasi awan.

Oleh karena itu, pemahaman mengenai jenis-jenis ancaman siber menjadi sangat penting agar individu dan organisasi dapat mengantisipasi serta mengembangkan strategi pertahanan yang efektif. Seperti dikemukakan oleh Ginni Rometty, mantan CEO IBM, "*Cybercrime is the greatest threat to every company in the world*." Pernyataan ini menggambarkan bahwa keamanan siber bukan lagi isu teknis semata, melainkan isu strategis yang menentukan keberlangsungan entitas di era *digital* (*DigitalDefynd*, 2024).

Ketika serangan ini dilancarkan secara terkoordinasi dari banyak perangkat yang terdistribusi (biasanya membentuk *botnet*), maka disebut *Distributed Denial-of-Service* (DDoS).

CISA (*Cybersecurity and Infrastructure Security Agency*) mendefinisikan DoS sebagai "serangan yang mencegah sistem komputer dari melayani pengguna komputer yang sah, atau yang menyebabkan penurunan kinerja sistem yang drastis" (CISA, n.d.). Bagaimana cara kerjanya?, serangan ini membanjiri target dengan jumlah lalu lintas data yang sangat besar atau permintaan yang memakan sumber daya, hingga melebihi kapasitasnya dan menyebabkan kelumpuhan.

2) Tipe-Tipe Serangan DDoS volume-*based attacks*: membanjiri *bandwidth* target. Contoh: UDP *Floods*, ICMP (*Ping*) *floods. protocol attacks:* mengeksploitasi kelemahan dalam protokol jaringan lapisan 3 atau 4. Contoh: SYN *Flood* (memanfaatkan proses TCP *handshake* yang tidak lengkap), *Ping of Death*.
3) *Application Layer Attacks*: menargetkan layer 7, menyerang aplikasi *web* secara langsung dengan permintaan tampak sah tetapi sangat intensif sumber daya. Contoh: HTTP *Flood* (membanjiri *server* dengan permintaan HTTP GET atau POST).

2. Perbandingan *Man-In-The-Middle* (MITM) dengan *Denial-of-Service* (DoS/DDoS)

Tabel 3.2: Perbandingan Antara *Man-In-The-Middle* (MITM) dengan *Denial-of-Service* (DoS/DDoS)

Aspek	*Man-In-The-Middle* (MITM)	*Denial-of-Service* (DoS/DDoS)
Tujuan Utama	Menyadap, mencuri, atau memanipulasi data	Melumpuhkan ketersediaan layanan
Sifat	Diam-diam (*stealthy*), pasif atau aktif	Terang-terangan (*overt*), destruktif
Korban	Individu atau grup spesifik (*targeted*)	Layanan atau infrastruktur (*broad*)
Dampak Utama	Kerahasiaan & integritas data terancam	Ketersediaan (*availability*) layanan hilang

Sumber: Diolah Penulis.

Serangan MITM (*Man-In-The-Middle*) dan DoS/DDoS memiliki tujuan, karakteristik, serta dampak yang berbeda dalam konteks keamanan siber. MITM berfokus pada pencurian, penyadapan, atau manipulasi data, dilakukan secara diam-diam dan menargetkan individu atau pihak tertentu. Dampak utamanya adalah terganggunya kerahasiaan dan integritas data.

Sebaliknya, serangan DoS/DDoS bertujuan untuk mengganggu atau melumpuhkan layanan sehingga tidak dapat diakses oleh pengguna. Serangan ini bersifat terang-terangan dan destruktif, menargetkan layanan atau infrastruktur secara luas. Dampak utama yang ditimbulkan adalah hilangnya ketersediaan (*availability*) layanan.

Secara keseluruhan, MITM mengancam aspek *Confidentiality* dan *Integrity*, sedangkan DoS/DDoS lebih mengancam aspek Availability dari sistem keamanan informasi. Kedua serangan ini menunjukkan pentingnya perlindungan komprehensif terhadap seluruh aspek CIA Triad (*Confidentiality, Integrity, Availability*) dalam keamanan siber.

3. Contoh Kasus dan Dampak

Melumpuhkan layanan perusahaan besar: serangan DDoS dapat membuat situs *e-commerce*, perbankan *online*, atau *platform cloud* tidak dapat diakses, mengakibatkan kerugian finansial langsung dan reputasi. Mengganggu Infrastruktur Kritikal: Serangan terhadap penyedia layanan internet atau DNS (seperti kasus Dyn) dapat mematikan akses internet untuk wilayah yang luas.

Sebagai pengalihan (*smokescreen*): serangan DDoS sering digunakan untuk mengalihkan perhatian tim keamanan IT sementara penyerang melancarkan serangan lain yang lebih berbahaya, seperti pencurian data. Contoh: Laporan Insiden Keamanan Siber Indonesia oleh BSSN (2022) mencatat peningkatan signifikan dalam serangan DDoS.

Laporan tersebut menyatakan, "Serangan DDoS masih menjadi ancaman utama dengan target utama sektor pemerintahan, jasa keuangan, dan teknologi informasi." (BSSN, 2022). Ini menunjukkan relevansi serangan ini di tingkat nasional.

Daftar Pustaka

BSSN (Badan Siber dan Sandi Negara). (2022). *Laporan Insiden Keamanan Siber Indonesia 2022.* [Sumber online, biasanya tersedia di website resmi BSSN].

Butarbutar, R. (2024). *Kejahatan Siber Terhadap Individu: Jenis dan Dampaknya.* Universitas Indonesia.

CISA (Cybersecurity and Infrastructure Security Agency). (n.d.). *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*. Diakses dari https://www.cisa.gov/uscert/ncas/tips/ST04-015.

CISA (Cybersecurity and Infrastructure Security Agency). (n.d.). *Cyber Threat Source Descriptions.* Diakses dari https://www.cisa.gov.

Cisco Umbrella. *Learn Cyber Threat Categories and Definitions. (n.d.).* Cisco Umbrella.

CompTIA. *What Is Cybersecurity | Types and Threats Defined. (n.d.).* comptia.org.

ConnectWise. *10 Common Cybersecurity Threats And Attacks: 2025 Update*. *(2025).* ConnectWise.

DigitalDefynd. (2024). *Inspirational Cybersecurity Quotes*. Diakses dari https://digitaldefynd.com/IQ/inspirational-cybersecurity-quotes.

ENISA (European Union Agency for Cybersecurity). (2023). *ENISA Threat Landscape Report.*

ENISA (European Union Agency for Cybersecurity). (n.d.). *Man-in-the-Middle (MitM) Attack.* Diakses dari https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/man-in-the-middle-mitm-attack.

Hyppönen, M. (2023). *Hyppönen's Law: If It's Smart, It's Vulnerable*. Diakses dari https://en.wikipedia.org/wiki/Mikko_Hypp%C3%B6nen.

IBM. (n.d.). *Jenis-Jenis Ancaman Siber*. Diakses dari https://www.ibm.com/id-id/think/topics/cyberthreats-types.

IBM. *Types of Cyberthreats. (n.d.).* Diakses dari IBM. IBM.

Imperva. *Cybersecurity Threats | Types & Sources. (n.d.).* Imperva.

Kaspersky. (2019). *What is a Man-in-the-Middle (MitM) Attack?.* Diakses dari https://www.kaspersky.co.id/resource-center/definitions/what-is-a-man-in-the-middle-attack.

Kaspersky. (n.d.). Securelist - Information about Viruses, Hackers, and Spam. Diakses dari https://securelist.com.

Massachusetts Government. *Know The Types of Cyber Threats. (n.d.).* Massachusetts Government.

Orsys. (2025). *10 Quotes on Cyber Security*. Diakses dari https://www.orsys.fr/orsys-lemag/en/10-quotes-on-cyber-security.

OWASP (Open Web Application Security Project). (2021). *ARP Spoofing.* Diakses dari https://owasp.org/www-community/attacks/ARP_Spoofing.

Saramuke, S. S. (2025). Ancaman Keamanan Siber dan Peran Aktor Non-Negara dalam Dinamika Globalisasi Digital. *Jurnal Syntax Idea.*

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford University Press.

Suharto, M. A. (2021). Konsep Cyber Attack, Cyber Crime, dan Cyber Warfare dalam Perspektif Hukum Internasional. *E-Journal Fakultas Hukum Universitas Mulawarman.*

Thomson Reuters Legal Solutions. *Types of Cybersecurity Threats. (2024, Oktober 4). l*egal.thomsonreuters.com.

Verizon. (2023). *Data Breach Investigations Report (DBIR).* Verizon Business.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet And The Launch of The World's First Digital Weapon*. Crown Publishing Group.

PROFIL PENULIS

Nasril Sany, S.Kom., M.Kom.

Minat penulis terhadap dunia ilmu komputer mulai tumbuh sejak tahun 1999. Ketertarikan tersebut mendorong penulis untuk menempuh pendidikan tinggi di STMIK Raharja (Universitas Raharja), memilih Jurusan Teknik Informatika (TI) dengan konsentrasi pada bidang *Software Engineering* (SE). Penulis berhasil menyelesaikan pendidikan jenjang Sarjana (S1) dan lulus pada tahun 2005. Guna memperdalam pemahaman dan kompetensinya di bidang teknologi informasi, penulis melanjutkan studi ke jenjang Magister (S2) di Universitas Budi Luhur, dan pada tahun 2017 berhasil meraih gelar Magister Ilmu Komputer, dengan peminatan pada Teknologi Sistem Informasi. Saat ini, penulis aktif sebagai dosen tetap di lingkungan pendidikan tinggi, tepatnya pada Program Studi Sistem Informasi di bawah naungan LLDIKTI Wilayah III, bertugas di Institut Teknologi PLN.

Dalam kapasitasnya sebagai tenaga pengajar, penulis mengampu berbagai mata kuliah yang berfokus pada pengembangan kompetensi teknis dan manajerial mahasiswa, antara lain: Konsep Sistem Informasi, Dasar Pemrograman, Sistem Informasi Manajemen, Struktur Data, Sistem Basis Data, Sistem Pendukung Keputusan, Jaringan Komputer dan UI/UX Desain. Selain mengajar, penulis juga aktif melakukan penelitian dan publikasi ilmiah serta menulis buku dalam bidang keilmuannya, seperti buku yang sudah terbit yaitu: Buku Pemodelan dan Visualisasi Data dan Buku Integrasi *Internet of Things* (IoT) *dan Embedded System dalam Era Digital*. Karya-karya ilmiah penulis dapat ditemukan dan diakses melalui portal akademik seperti SINTA (*Science and Technology Index*) dan *Google Scholar*. Dengan latar belakang akademik yang kuat dan pengalaman mengajar yang luas, penulis terus berkomitmen untuk berkontribusi dalam pengembangan ilmu pengetahuan dan teknologi, serta membimbing generasi muda dalam menghadapi tantangan dunia *digital* yang semakin kompleks.

Email Penulis: nasrilsanypenulis@gmail.com.

BAB 4
SCANNING & ENUMERATION

Haryanto, S.Kom., M.M., M.TI.
Universitas Raharja

Tujuan *Scanning* dan Enumerasi

Scanning dan enumerasi adalah dua aktivitas penting dalam keamanan siber yang membantu mengidentifikasi potensi ancaman dan kerentanan keamanan dalam jaringan komputer. *Scanning* adalah proses mengirimkan permintaan ke sistem target untuk mengumpulkan informasi tentang topologi jaringan, portal yang terbuka, dan layanan yang sedang berjalan.

Enumerasi adalah proses menggunakan informasi yang dikumpulkan selama *Scanning* untuk mengidentifikasi detail spesifik tentang sistem target, seperti sistem operasi, aplikasi, dan akun pengguna. Dengan menggabungkan informasi yang dikumpulkan dari *Scanning* dan enumerasi, penguji dapat membangun profil komprehensif sistem target, dan menggunakan informasi ini untuk mengembangkan strategi penyerangan.

Dalam uji penetrasi, terdapat batasan tersirat. Tergantung pada luas dan cakupan pengujian anda, anda mungkin dibatasi untuk menguji sejumlah atau jenis *host* tertentu, atau anda mungkin bebas menguji apa pun yang dimiliki atau dioperasikan oleh klien anda. Untuk memindai dan mengidentifikasi sistem dengan benar, anda perlu mengetahui kondisi akhir untuk penilaian anda. Setelah *Scanning* dan enumerasi selesai, anda harus:

Memastikan bahwa alamat IP yang ditemukan dalam fase pengintaian dapat dijangkau. Ini adalah fase "vitalitas" pengintaian. Mampu mengidentifikasi tujuan dan jenis sistem target, yaitu, apa itu dan apa yang mereka lakukan. Memiliki informasi spesifik tentang versi layanan yang berjalan pada sistem. Memiliki daftar target dan layanan yang ringkas yang akan secara langsung dimasukkan ke dalam aktivitas uji penetrasi lebih lanjut.

Scanning Target

Langkah pertama kami setelah melakukan *footprinting* target adalah memulai *Scanning*. Pada tahap *footing*, kami mengumpulkan berbagai macam informasi; namun, dengan *Scanning*, kami berbicara tentang upaya yang jauh lebih terfokus. Singkatnya, *Scanning* adalah proses menemukan sistem di jaringan dan melihat *port* dan aplikasi terbuka apa yang mungkin sedang berjalan.

Dengan *footprinting*, kami ingin mengetahui seberapa besar jaringan tersebut dan beberapa informasi umum tentang susunannya: dalam *Scanning*, kami akan benar-benar masuk ke jaringan dan mulai menyentuh setiap perangkat untuk mengetahui lebih lanjut tentangnya. Dalam *Scanning*, ada tiga jenis utama *Scanning* jaringan, *scanning port*, dan *Scanning* kerentanan serta serangkaian langkah dasar yang harus diikuti oleh peretas etis.

Namun, penting untuk diingat bahwa sebagaimana langkah-langkah dalam keseluruhan proses peretasan dapat saling berpadu, langkah-langkah ini hanyalah panduan umum dan bukan seperangkat aturan baku yang harus diikuti. Saat anda sedang bekerja, akan muncul situasi dan keadaan yang mungkin memaksa anda mengubah urutannya.

Terkadang proses menyelesaikan satu langkah akan langsung menyatu dengan langkah lainnya. Jangan khawatir ikuti saja alurnya dan selesaikan pekerjaan anda. Langkah-langkah untuk metodologi *Scanning* adalah:

1. **Identifikasi Sistem yang Aktif**: sesuatu yang sederhana seperti ping dapat memberikan informasi ini. Ini akan memberi anda daftar sistem yang aktif di subnet jaringan anda.
2. **Temukan *Port* yang Terbuka**: setelah anda mengetahui alamat IP mana yang aktif, temukan port mana yang sedang mereka dengarkan.
3. **Identifikasi OS dan Layanannya**: *banner grabbing* dan sidik jari OS akan memberitahu anda sistem operasi apa yang ada di mesin dan layanan apa yang dijalankannya.
4. **Pindai Kerentanan**: lakukan pemeriksaan yang lebih terfokus pada kerentanan yang belum ditambal pada mesin-mesin ini (Matt Walker, 2012).

Mengidentifikasi Mesin Aktif

Pada langkah pertama setelah *footprinting*, anda perlu mencari tahu alamat IP mana yang benar-benar "aktif". Cara termudah dan paling sederhana untuk melakukannya adalah dengan memanfaatkan protokol yang tertanam di tumpukan setiap perangkat yang mendukung TCP/IP di dunia ICMP (I*nternet Control Message Protocol*).

a. *Nmap*

Scanners port menerima target atau rentang sebagai input, mengirimkan kueri ke *port* tertentu, dan kemudian membuat daftar respons untuk setiap *port*. Pemindai yang paling populer adalah *Nmap*, yang ditulis oleh Fyodor dan tersedia di *www.insecure.org*. Alat serbaguna Fyodor telah menjadi standar di kalangan penguji pena dan auditor jaringan.

Tujuan buku ini bukanlah untuk mengajarkan anda semua cara menggunakan *Nmap*; namun, kami akan berfokus pada beberapa jenis dan opsi *Scanning* yang berbeda, untuk memaksimalkan waktu *Scanning* anda dan mengembalikan informasi terbaik guna meningkatkan kedalaman serangan anda (Codi A Cochran, 2024).

Nmap USAGE
How to use:
nmap [*Scan Type*(s)] [*Options*] Target(s)
Input fields:
[*Scan Type*] *is the type of scan to perform. Different scan options are available and are*
discussed throughout this chapter.
[*Options*] *include a wide variety of configuration options including* DNS *resolution, use of*
traceroutes, and more.
Target is the target specification which can be a single host, a list of host names or IPs,
or a full network.
Output:
Displays host information to the screen depending on scan type and options selected.
including accessibility of the host, active ports, and fingerprint data. There are also options
available to output this data to a file.
Typical output: (*extract*)
root@bt:~/*nmap_scans*# *nmap-sn--send*-ip 192.168.1.0/24-oA
nmap-sweep.
Starting Nmap 5.30BETA1 (http://nmap.org) at 2010-08-01 10:17 CDT.
Nmap scan report for 192.168.1.1
Host is up.

Nmap scan report for 192.168.1.100.
Host is up (0.061s *latency*).
MAC *Address*: 00:0C:29:67:63:F5 (VM*ware*).
Nmap scan report for 192.168.1.110.
Host is up (0.0047s *latency*).
MAC *Address*: 00:0C:29:A2:C6:E6 (VM*ware*).
Nmap done: 256 IP *addresses* (3 *hosts up*) *scanned in* 89.75 *Seconds*.

b. *Nmap*: *Ping Sweep*

Sebelum memindai target aktif, pertimbangkan untuk menggunakan fungsi *ping sweep Nmap* dengan opsi -sn. Opsi ini tidak akan memindai *port* target, tetapi akan melaporkan target mana yang aktif. Ketika dipanggil sebagai *root* dengan *nmap-sn* ip_*address, Nmap* akan mengirimkan paket ICMP *echo* dan timestamp serta paket TCP SYN dan ACK untuk menentukan apakah suatu *host* aktif.

Jika alamat target berada di jaringan Ethernet lokal, Nmap akan secara otomatis melakukan Scanning ARP alih-alih mengirimkan paket dan menunggu balasan. Jika permintaan ARP berhasil untuk suatu target, permintaan tersebut akan ditampilkan. Untuk mengesampingkan perilaku ini dan memaksa Nmap untuk mengirimkan paket IP, gunakan opsi -*send*-ip.

Jika *sweep* perlu melewati *firewall*, mungkin juga berguna untuk menggunakan *Scanning* TCPACK bersamaan dengan Scanning TCP SYN. Menentukan -PA akan mengirimkan satu paket TCP ACK yang dapat melewati konfigurasi *firewall stateful* tertentu yang akan memblokir paket SYN kosong ke *port* tertutup. Pada rilis *Nmap* sebelumnya, jenis *Scanning* ini dipanggil menggunakan opsi -sP.

Dengan memahami teknik mana yang berguna untuk lingkungan mana, anda meningkatkan kecepatan Scanning anda. Ini mungkin bukan masalah besar saat memindai beberapa sistem, tetapi saat memindai beberapa jaringan /24, atau bahkan /16, Anda mungkin memerlukan waktu tambahan ini untuk pengujian lainnya. Dalam contoh yang diilustrasikan

sapuan ping standar adalah yang tercepat untuk lingkungan khusus ini, tetapi hal itu mungkin tidak selalu terjadi.

c. *Nmap*: Opsi ICMP

Jika *nmap* tidak dapat melihat target, ia tidak akan memindai target kecuali opsi -Pn (jangan *ping*) digunakan. Opsi ini dipanggil menggunakan opsi -P0 dan -PN pada rilis Nmap sebelumnya. Penggunaan opsi -Pn dapat menimbulkan masalah karena *nmap* akan mencoba memindai setiap port target, meskipun target tidak aktif, yang dapat membuang waktu.

Untuk mencapai keseimbangan yang baik, pertimbangkan untuk menggunakan opsi -P untuk memilih jenis perilaku ping lain. Misalnya, opsi -PP akan menggunakan permintaan stempel waktu ICMP dan opsi -PM akan menggunakan permintaan netmask ICMP. Sebelum anda melakukan *Scanning* penuh pada rentang jaringan, mungkin ada baiknya melakukan beberapa pengujian terbatas pada alamat IP yang diketahui, seperti *server web*, DNS, dan sebagainya, sehingga anda dapat menyederhanakan *Scanning ping* dan mengurangi jumlah total paket yang dikirim, serta waktu yang dibutuhkan untuk *Scanning* (Matt Walker, 2012).

d. Nmap: Opsi Keluaran

Menangkap hasil *Scanning* sangatlah penting, karena anda akan merujuk pada informasi ini nanti dalam proses pengujian, dan bergantung pada kebutuhan klien anda, anda mungkin mengirimkan hasilnya sebagai bukti kerentanan. Cara termudah untuk menangkap semua informasi yang dibutuhkan adalah dengan menggunakan *flag* -oA, yang mengeluarkan hasil *Scanning* dalam tiga format berbeda secara bersamaan: teks biasa (.*nmap*), teks yang dapat di-*greppable* (.*gnmap*), dan XML (.xml). Format .*gnmap* sangat penting untuk diperhatikan, karena jika anda perlu menghentikan *Scanning* dan melanjutkannya di kemudian hari, *Nmap* akan meminta berkas ini untuk melanjutkannya, dengan menggunakan *switch-resume*.

Daftar Pustaka

Codi A Cochran. (2024). *Cybersecurity Essentials Scanning And Enumeration, Apress, Berkeley.* https://booksite.elsevier.com/samplechapters/9781597496278/Chapter_3.pdf.

Dunn Cavelty, M., & Wenger, A. (2020). Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, And Networked Science. *Contemporary Security Policy*, 41(1), 5–32.https://doi.org/10.1080/13523260.2019.1678855.

Echlin, P. (2011). *Handbook of Sample Preparation For Scanning Electron Microscopy And X-Ray Microanalysis*. Springer Science & Business Media.

Matt Walker. (2012). CEH Certified Ethical Hacker EXAM GUIDE The McGraw-Hill Companies. All Rights Reserved. *Printed In The United States of America*.

PROFIL PENULIS

Haryanto, S.Kom., M.M., M.TI.

Penulis memiliki kepakaran dibidang Keuangan Perusahaan. Hal tersebut membuat penulis memilih untuk melanjutkan pendidikan ke Universitas Budi Luhur Jurusan Komputer Akuntansi dan berhasil menyelesaikan studi S1 di pada tahun 2006. Dua tahun kemudian, penulis menyelesaikan studi S2 di Magister Manajemen Universitas Budi Luhur, penulis menyelesaikan S2 Magister Teknologi Informasi di Universitas Raharja. Penulis memperdalam dalam ilmu marketing dan memasarkan produk-produk yang berkaitan dengan mesin industri. Perusahaan yang dipimpinnya Bersama temannya dalam mengembangkan perusahaan, PT. Multi Sinar Teknik dan untuk mengembangkan ilmu sebagai dosen profesional, penulis pun aktif sebagai peneliti di bidang lainnya dan menulis beberapa artikel artikel yang telah diterbitkan dan Beberapa penelitian yang telah dilakukan. Selain peneliti, penulis juga aktif menulis buku dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara yang sangat tercinta ini. Atas dedikasi dan kerja keras dalam menulis buku, Penulis aktif dalam Strategi *Marketing* yang telah dijalankan dalam perusahaan menjadi strategi dan perencanaan sebuah pemasaran serta organisasi pemasaran.

Email Penulis: haryanto@raharja.info.

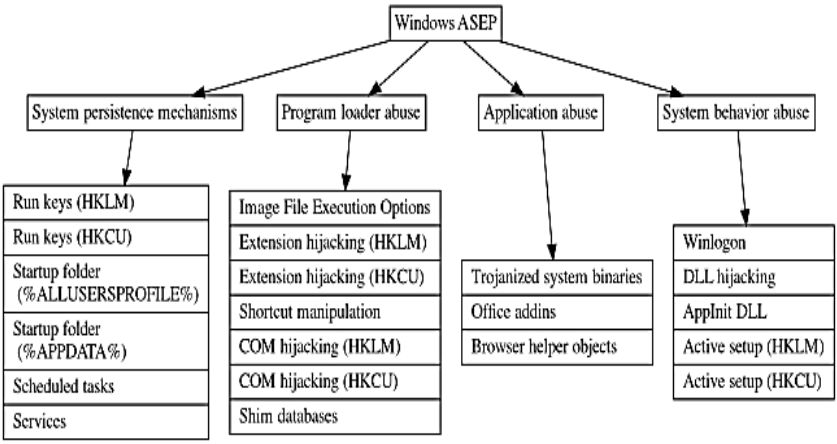
BAB 5
PERSISTENCE DAN *BACKDOOR*

Rosmawati Dwi, S.T., M.Kom.
Universitas Raharja

Persistence

Dalam konteks keamanan siber, *persistence* dapat diartikan sebagai kemampuan atau mekanisme untuk menjaga dan mempertahankan akses ke dalam sistem yang telah disusupi. Aktivitas ini bertujuan untuk mempertahankan akses jangka panjang tanpa diketahui oleh sistem yang disusupi (Gittins and Soltys 2020).

Berikut taksonomi mekanisme *persistence* yang telah dianalisis berdasarkan temuan yang terjadi di seluruh dunia sampai dengan saat ini. Taksonomi ini khusus untuk mekanisme *persistence* di OS *windows*, yang dikenal dengan istilah "*Windows Auto-Start Extensibility Points (ASEP)*(Uroz and Rodríguez 2019)".



Gambar 5.1: *Windows Auto-Start Extensibility Points* (ASEP), Taksonomi Mekanisme *Persistence Windows*

Sumber: *A Taxonomy for Threat Actors' Persistence Techniques* (Villalón-Huerta, Marco-Gisbert, and Ripoll-Ripoll 2022).

1. *System Persistence Mechanisms*

Pada kategori ini, penyusup mencoba menggunakan celah keamanan dari mekanisme yang sudah diketahui umum disediakan oleh *windows* untuk menjalankan sebuah program, *task* atau *system service*, antara lain:

a. *Run Keys*

Berdasarkan dokumen panduan *Microsoft* tahun 2025 (*microsoft doc*-Jalankan dan Jalankan Kunci Registri *RunOnce*-

Win32 *apps _ Microsoft Learn* n.d.), *run keys registry* berfungsi untuk membuat program berjalan saat pengguna masuk. Terdapat 2 jenis run keys yaitu, *Run* dan *Run0nce*.

Run dapat membuat program berjalan setiap kali pengguna *Login*, sedangkan *Run0nce* hanya dapat dieksekusi sekali lalu otomatis kunci tersebut terhapus dari *registry*. Berikut empat kunci registry window, yaitu sebagai berikut:

1) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run.
2) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce.
3) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run.
4) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce.

Untuk dapat melakukan penyusupan secara *persistence* dalam *run keys* baik HKLM maupun HKCU, penyusup biasanya menanamkan *malware*/*worm* yang dapat mengeksekusi di level *run key registry. Malware* tersebut biasanya sudah di level *root system* sehingga segala kredential *administrator* sudah dimiliki dan dapat mereplikasi saat *system reboot* kembali. Cara untuk mengetahui apakah *run key* sebuah *system* pernah/sedang disusupi oleh *persistence malware* yaitu dengan melakukan *memory forensics.*

b. *Start-up Folders*

Start-up folder adalah *folder* yang berisi *shortcut* dari program-program atau aplikasi yang akan selalu dijalankan setiap menyalakan sebuah *windows* sistem. Terdapat dua konfigurasi startup folder pada *windows*, yaitu %APPDATA% dan %ALLUSERSPROFILE%. Dua konfigurasi *start-up folder* tersebut terdapat pada subpath *Microsoft**Windows**Start Menu**Programs**Startup*.

Penyusup menaruh *malware* di *subpath* tersebut agar setiap *login user* atau masuk ke dalam sistem windows, otomatis *malware* tersebut dijalankan. Jika kita mencurigai adanya

persistence attack pada *start-up folder* kita, bisa menggunakan *disc forensic analysis.*

c. *Scheduled Task*

Berdasarkan dokumen panduan *windows* (*Task Scheduler for developers*-Win32 *apps* | *Microsoft Learn* n.d.), *Scheduled task* merupakan task atau program yang otomatis dijalankan oleh *scheduler* saat memenuhi kriteria yang sebelumnya telah ditetapkan untuk program tersebut.

Task tersebut harus berupa XML file yang ditempatkan pada *path*: %SystemRoot%\System32\Tasks. Untuk dapat mengakses *path* tersebut, *user* harus memiliki akses sebagai *system administrator*. Berikut beberapa kriteria yang bisa diset oleh *developer* saat akan menaruh *task* pada *path scheduled task*:

1) Saat waktu tertentu (jadwal harian, mingguan, atau bulanan).
2) Saat komputer *idle*.
3) Saat *task* di-*register.*
4) Saat *system reboot.*
5) Saat kejadian spesifik muncul, missal saat membuka *word*, atau saat *folder* tertentu di klik.
6) Saat *user log in*.
7) Saat *server* berubah *session.*

Sebuah *system* yang telah disusupi oleh *backdoor*, dan *backdoor* tersebut dapat mengakses *path scheduled task* serta menaruh *malware* pada *path* tersebut, maka saat kondisi sistem memenuhi kriteria yang dimaksud, maka *malware* tersebut akan otomatis dijalankan oleh *system*.

d. *Services*

Window service adalah program *background* yang berjalan tanpa perlu interaksi dari *user*. Seperti Scheduled *task, service* bisa dieksekusi jika memenuhi kondisi dengan kriteria tertentu. Perbedaannya terletak pada cara kerjanya. Jika *scheduled task* merupakan program yang berjalan dengan jadwal tertentu, dan setelah selesai tugasnya, program tersebut berhenti sampai dengan jadwal berikutnya. Namun, *services* merupakan program

yang berjalan secara terus menerus secara independen selama system menyala. Contohnya: *web server* (IIS), w*indows update,* dll.

2. *Program Loader Abuse*

Pada mekanisme *persistence program loader abuse* ini, penyusup meng-eksploitasi program biasa yang digunakan oleh user, untuk menjalankan program lain (*malware*) yang tidak disadari oleh pengguna. Beberapa teknik yang biasa digunakan antara lain:

a. *Image File Execution Option*

Image File Execution Option (IFEO) adalah fitur *windows* yang memungkinkan pembuat program untuk mengeksekusi program langsung saat sedang *debug* (Al-Janabi 2010). Cara mengaktifkan IFEO yaitu sebagai berikut:

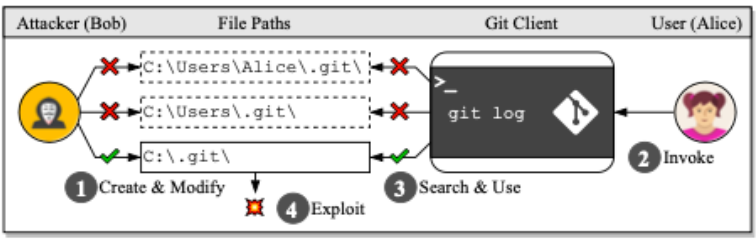
1) *Start Registry Editor*
   a) Klik *start*.
   b) Klik *run*.
   c) Ketik *regedit.exe*
2) Meletakkan *registry key* pada *path* HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion \Image File Execution Options.
3) Penamaan *registry key* harus sama dengan *source program* yang akan dieksekusi, contoh: program *excel.exe* maka buat key dengan cara klik kanan: *New-key*, lalu beri nama *key*: *excel.exe*.
4) Dalam *box* "Value data", ketik *path* dari *debugger* yang akan diakses, contoh: C:\Windows\System32\calc.exe.

Celah keamanan pada fitur ini terletak pada tidak adanya verifikasi *program debugger* yang dimaksud, sehingga saat aplikasi *excel* dibuka, otomatis system akan mengeksekusi juga program kalkulator. Untuk *persistence* tipe ini memang hanya akan tereksekusi jika program utama dipanggil, sehingga biasanya *persistence* tipe ini menyerang program-program yang umum digunakan orang seperti *browser, office*, dll. Untuk mengakses fitur ini memang memerlukan *user administrator* karena menggunakan *registry editor,* namun sekali sistem

administrator berhasil disusupi, maka dapat dengan leluasa menggunakan fitur ini.

b. *Extention Hijacking*

Extention hijacking merupakan teknik *persistence* dengan cara mengganti program yang dijalankan saat mengakses suatu *file* tertentu misalnya .docx, .pdf, .pptx, .Git, .txt, dll. Program pengganti ditanamkan melalui *backdoor* ke dalam *windows registry* dengan *subkey*:
HKCU\Software\Classes\Applications.
HKLM\Software\Classes\Applications.



Gambar 5.2: Teknik *File Extension Hijacking* Pada *File .Git*
Sumber: *File Hijacking Vulnerability*: *The Elephant In The Room* (Yu *et al.* 2024).

c. *Shortcut Manipulation*

Cara kerja *Shortcut Manipulation* mirip seperti *Extension Hijacking*, hanya saja untuk *shortcut manipulation, object* yang disusupi yaitu *file shortcut* yang memang sudah ada sebelumnya dalam sistem. Dengan menempelkan *backdoor* pada suatu *shortcut*, menyebabkan saat kita mengeksekusi *shortcut* tersebut, *backdoor* mengalihkan ke program lain.

Cara membuat *shortcut manipulation* cukup sederhana, tidak memerlukan akses *administrator*. Menempelkan program asli dengan program tidak dikenal dengan karakter ';', sehingga saat *shortcut* di klik, program yang terpanggil langsung kedua program tadi. Kelemahan dari *shortcut manipulation* yaitu hanya dapat dijalankan saat *user* mengakses *shortcut* yang disusupi, serta dapat dengan mudah dideteksi melalui *disk forensic analysis*.

Daftar Pustaka

Al-Janabi, Rana Jumaa Surayh. (2010). Malware Avoidance Using Redirection Technique. *Journal of Al-Nahrain University Science* 13(3): 178–84. doi:10.22401/jnus.13.3.29.

Gittins, Zane, and Michael Soltys. (2020). Malware Persistence Mechanisms. *Procedia Computer Science* 176: 88–97. doi:10.1016/j.procs.2020.08.010.

Guo, Wenbo, Lun Wang, Xinyu Xing, Min Du, and Dawn Song. (2019). TABOR: A Highly Accurate Approach to Inspecting and Restoring Trojan Backdoors in AI Systems. http://arxiv.org/abs/1908.01763.

Matthew McWhirt, Jon Erickson, DJ Palombo. (2017). To SDB, Or Not To SDB: FIN7 Leveraging Shim Databases for Persistence | FireEye Inc. *FireEye Blogs, Threat Research*. https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html.

Microsoft Doc-Jalankan Dan Jalankan Kunci Registri RunOnce - Win32 Apps _ Microsoft Learn.

Office Add-Ins Platform Overview - Office Add-Ins | Microsoft Learn. https://learn.microsoft.com/en-us/office/dev/add-ins/overview/office-add-ins.

Park, Beomsoo, Sungjin Hong, Jaewook Oh, and Heejo Lee. (2005). Defending a Web Browser against Spying with Browser Helper Objects. *Lecture Notes in Computer Science* 3495: 638–39. doi:10.1007/11427995_85.

Sasmoko, Dani, and Galih Setiawan. (2020). Istilah Keamanan Sistem Informasi Dalam Film 'Who Am I–No System Is Safe (2014). *Academia.Edu* (2014). https://www.academia.edu/download/62204073/GalihS_Istilah_Keamanan20200226-88045-fbxni1.pdf.

Sopaheluwakan, Christian Ronaldo, and Dian Widiyanto Chandra. (2020). Anti-WebShell PHP Backdoor Scanner Pada Linux Server. *ILKOM Jurnal Ilmiah* 12(2): 143–53.

doi:10.33096/ilkom.v12i2.596.143-153.

Task Scheduler for Developers-Win32 Apps | Microsoft Learn. https://learn.microsoft.com/en-us/windows/win32/taskschd/task-scheduler-start-page.

Uroz, Daniel, and Ricardo J. Rodríguez. (2019). Characteristics and Detectability of Windows Auto-Start Extensibility Points in Memory Forensics. *Digital Investigation* 28: S95–104. doi:10.1016/j.diin.2019.01.026.

Villalón-Huerta, Antonio, Hector Marco-Gisbert, and Ismael Ripoll-Ripoll. (2022). A Taxonomy for Threat Actors' Persistence Techniques. *Computers and Security* 121. doi:10.1016/j.cose.2022.102855.

Yu, Chendong, Yang Xiao, Jie Lu, Yuekang Li, Yeting Li, Lian Li, Yifan Dong, et al. (2024). File Hijacking Vulnerability: The Elephant in the Room. (March). doi:10.14722/ndss.2024.23038.

PROFIL PENULIS

Rosmawati Dwi, S.T., M.Kom.

Menjadi Ibu dari tiga orang anak serta sekaligus aktif bekerja di bidang IT Perbankan tidak membuat Penulis ini berhenti untuk berkarya, justru hal tersebut yang memotivasi penulis untuk menyalurkan ilmu dan ketertarikan-nya dalam bidang akademik untuk menulis buku ajar ini. Kesenangannya untuk mengajar di sela-sela kesibukannya sebagai seorang profesional dan seorang ibu menurun dari ibunya yang merupakan seorang guru SD dan kakeknya yang juga merupakan seorang guru.

Lahir di Tasikmalaya 35 tahun silam, tepatnya tanggal 16 Desember 1987 dan merupakan anak kedua dari tiga bersaudara dari pasangan Ayah (Alm) Akhmad Suhro dan Ibu Oon Sapronah. *Background* IT penulis berasal dari Pendidikan S1 yang Penulis emban selama 3,5 di prodi Teknik Telekomunikasi Universitas Telkom (dahulu: IT Telkom) di kota Bandung dan lulus di tahun 2010 dengan predikat *cumlaude*. Setelah itu Penulis meneruskan studi S2 pada tahun 2015-2017 di *Swiss German University* dengan mengambil jurusan IT *Security* sambal tetap bekerja di Perusahaan IT sebagai *developer*. Dalam bidang IT, penulis memiliki ketertarikan dalam bidang *Image Processing*, Kriptografi dan *biometric*. Sejalan dengan itu, penelitian-penelitian yang pernah dilakukannya antara lain autentikasi palmprint berbasis *image processing* dan penerapan enkripsi *image* (EVCS) pada *palmprint recognition*.

Email Penulis: rosmawati.dwi@gmail.com.

BAB 6
HARDENING SISTEM OPERASI DAN APLIKASI

Martono, S.Pd.Kim., M.TI.
Universitas Raharja

Pendahuluan

Hardening Sistem Operasi atau *Hardening* Sistem Operasi sangat penting untuk meningkatkan keamanan dengan meminimalkan "permukaan serangan", yang mengurangi kerentanan yang dapat dieksploitasi oleh penjahat siber.

Proses ini melibatkan penghapusan atau penonaktifan fitur dan layanan yang tidak diperlukan, penerapan kontrol akses yang ketat, dan konfigurasi sistem agar lebih tangguh terhadap serangan siber seperti pelanggaran data dan *malware*. Pada akhirnya, hal ini menurunkan risiko pencurian data, akses tidak sah, dan penyusupan sistem, sehingga sistem menjadi lebih tangguh dan sulit ditembus.

Hardening Sistem Operasi merupakan proses pengamanan sistem dengan mengurangi permukaan serangan dan jumlah titik masuk yang potensial bagi penyerang. Hal ini dicapai bisa dengan cara menghapus atau menonaktifkan beberapa fitur, layanan dan konfigurasi yang tidak diperlukan yang dapat dieksploitasi oleh peretas atau *malware*.

Hardening akan melibatkan manajemen konfigurasi yang tepat saat menerapkan aplikasi dan sistem baru. Meskipun mengizinkan OS dan aplikasi untuk diinstal dan dijalankan dengan konfigurasi bawaan tanpa *Hardening* dapat menghemat waktu akses, performa dan tampak lebih nyaman. Penerapan dan penggunaan tanpa hardening ini dapat menimbulkan risiko yang signifikan bagi sistem secara keseluruhan.

Memperbarui Sistem Operasi

Sebuah sistem operasi mungkin akan banyak kerentanan keamanan dan *bug* perangkat lunak saat pertama kali dirilis. *Vendor*, seperti *Red Ha*t dan *Microsoft*, menyediakan pembaruan Sistem Operasi untuk memperbaiki kerentanan dan *bug* ini.

Bahkan, banyak organisasi konsultan menyarankan agar organisasi tidak membeli dan mengimplementasikan Sistem Operasi baru hingga pembaruan pertama tersedia. Dalam kebanyakan kasus, pembaruan pertama akan memperbaiki banyak masalah yang dihadapi pada rilis pertama sistem operasi tersebut.

Untuk memastikan perlindungan aplikasi dan informasi yang digunakannya, perlu ditambahkan kontrol keamanan tambahan untuk

memperkuat sistem operasi dan aplikasi. Penggunaan konfigurasi bawaan tidak memberikan tingkat keamanan yang memadai bagi sebagian besar organisasi.

Perbedaan *Hardening* Sistem dan *Hardening* Sistem Operasi

Sebelum membahas tentang *hardening* sistem operasi dan Aplikasi tidak ada salahnya kita membahas tentang *Hardening* Sistem. *Hardening system* adalah proses luas untuk mengamankan keseluruhan sistem sementara *hardening* sistem operasi merupakan komponen dari proses tersebut yang secara khusus berfokus pada pengamanan inti Sistem Operasi itu sendiri.

Hardening sistem mencakup pengamanan semua lapisan sistem, termasuk OS, aplikasi, dan jaringan, sedangkan *Hardening* OS berfokus pada penghapusan layanan yang tidak perlu, perbaikan kerentanan, dan konfigurasi pengaturan keamanan di tingkat sistem operasi saja

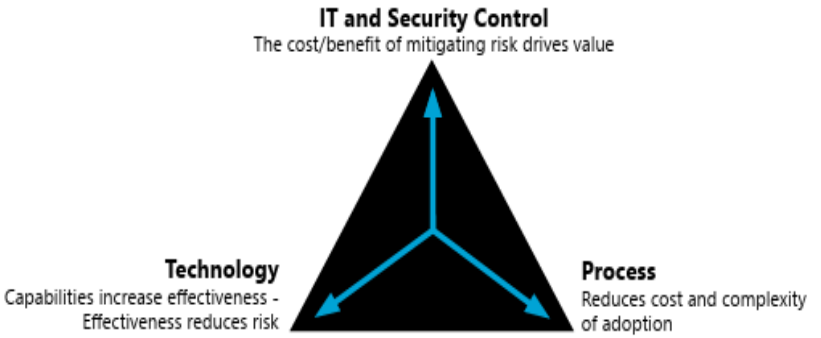
Jenis-Jenis *Hardening System*

Hardening sistem sebaiknya diterapkan pada setiap lapisan infrastruktur TI perusahaan, mulai dari *server* hingga jaringan, bahkan titik akhir. Ada lima kategori yang dapat dibagi menjadi proses ini: *Server Hardening. Software Hardening, Operating System Hardening, Database Hardening*, dan *Network Hardening*.

Gambar 6.1: Jenis-Jenis *Hardening System*
Sumber: https://heimdalsecurity.com/blog/wp-content/uploads/2022/12/system-hardening-types-diagram.jpg.

program tersebut untuk melakukan hal-hal tertentu di *server*, berbeda dengan *Hardening* aplikasi yang berfokus pada pengamanan aplikasi standar dan pihak ketiga.

Hardening aplikasi adalah proses keamanan yang mengamankan aplikasi dari serangan dengan menghilangkan kerentanan dan menambahkan lapisan pertahanan. Hal ini dicapai melalui teknik-teknik seperti pengaburan kode, enkripsi, dan pemantauan *runtime* untuk mempersulit peretas dalam merekayasa balik, merusak, atau mengeksploitasi aplikasi. Dengan memperkuat aplikasi, organisasi melindungi data sensitif, kekayaan intelektual, dan reputasi merek. Tiga dimensi *hardening* aplikasi:



Gambar 6.3: Tiga Dimensi *Hardening* Aplikasi

Sumber: http://profs.sci.univr.it/~giaco/download/Watermarking-Obfuscation/Reverse_engineering_risk_assessment_for_distribution.

Gambar yang anda berikan menggambarkan kerangka kerja dimana Teknologi , Proses , dan Kontrol TI dan Keamanan berinteraksi untuk mendorong nilai melalui mitigasi risiko:

1. Kemampuan Teknologi meningkatkan efektivitas, yang pada gilirannya mengurangi risiko. Hardening Aplikasi termasuk dalam aspek teknologi karena melibatkan penerapan langkah-langkah dan perangkat keamanan teknis.
2. Proses ini membantu mengurangi biaya dan kompleksitas penerapan langkah-langkah keamanan ini. Hardening Aplikasi adalah proses sistematis dan metodis yang melibatkan audit, perencanaan, implementasi, dan pemantauan.

Daftar Pustaka

https://www.almabetter.com/bytes/articles/types-of-operating-system.

https://www.beyondtrust.com/resources/glossary/systems-hardening.

https://calcomsoftware.com/os-hardening-20-best-practices/.

https://www.cyber.gc.ca/en/guidance/top-10-security-actions-number-4-harden-operating-systems-and-applications-itsm10090.

https://heimdalsecurity.com/blog/system-hardening/.

https://linfordco.com/blog/operating-system-hardening/.

https://www.pynetlabs.com/what-is-device-hardening/.

http://profs.sci.univr.it/~giaco/download/Watermarking-Obfuscation/Reverse_engineering_risk_assessment_for_distribution.pdf.

PROFIL PENULIS

Martono, S.Pd.Kim., M.TI.

Ketertarikan penulis pada bidang komputer awalnya hanya karena hobi dan iseng-iseng. Sambil menyelesaikan Pendidikan Kimia jenjang Diploma 3 di IKIP Jakarta pada saat itu penulis juga mengikuti pelatihan elektronika komputer. Belajar tentang jaringan komputer dimulai dari era *Novell Netware* dan *Microsoft NT 4.0* pada saat jaringan LAN yang masih populer menggunakan *Cable Coaxial* hingga kini era jaringan menggunakan *Wifi* dan *Fiber Optics*, hal tersebut lebih karena tuntutan pekerjaan.

Pendidikan D3 diselesaikan di IKIP Jakarta dan S1 diselesaikan di Universitas Terbuka pada tahun 2006 masih pada Jurusan yang sama yakni Pendidikan Kimia. Penulis melanjutkan Pendidikan S2 di STMIK Raharja pada program studi Teknik Informatika dan selesai pada tahun 2017. Awalnya penulis bekerja di Perusahaan yang merupakan *vendor* di bidang Teknologi Informasi yang melayani lembaga pendidikan dan perusahaan. Kemudian penulis bergabung dengan perusahaan Teknologi Informasi yang memberikan pelatihan-pelatihan ke sekolah-sekolah dan juga mengembangkan *Software-software* Pendidikan dan Pelatihan Robotika. Dari sini penulis akhirnya banyak melakukan eksplorasi *software, Network*, Mikrokontroler dan Robotika serta terlibat baik secara langsung maupun tidak langsung dalam pengembangan *software.* Beberapa tulisan ringan ditulis dalam bentuk blog dan sering menggunakan nickname martonokita. Adapun tulisan ilmiahnya telah diterbitkan dalam beberapa buku dan dalam beberapa Jurnal Ilmiah. Selain memberikan pelatihan, penulis juga mengajar di SMKN 4 Depok, Universitas Raharja dan beberapa perguruan tinggi.

Email Penulis: martono@raharja.info.

BAB 7
MENCEGAH DAN MENANGKAL SERANGAN WEB

Lilis Supratman, M.Si.
Universitas Pakuan

Pendahuluan

Keamanan *web* menjadi aspek kritis dalam pengembangan dan pengelolaan sistem informasi modern. Seiring meningkatnya ketergantungan terhadap aplikasi *web* untuk transaksi, komunikasi, hingga penyimpanan data, ancaman terhadap web juga tumbuh secara eksponensial.

Serangan seperti SQL *injection, cross-site scripting* (XSS), *Distributed Denial of Service* (DDoS), dan *session hijacking* telah menjadi tantangan utama dalam dunia keamanan siber (Stuttard & Pinto 2011). Oleh karena itu, strategi untuk mencegah sekaligus merespons serangan sangat penting dalam mempertahankan integritas, ketersediaan, dan kerahasiaan sistem informasi (Anderson 2020).

1. **Definisi Keamanan *Web* Dan Pentingnya Pertahanan Aplikasi *Web***

   Keamanan *web* mencakup praktik, teknologi, dan proses untuk menjaga integritas, kerahasiaan, dan ketersediaan aplikasi web serta data yang diprosesnya. Dalam konteks aplikasi modern yang seringkali terdiri dari *front-end*, API, *microservices*, dan penyimpanan *cloud*, kerentanan kecil pada lapisan input, otentikasi, atau konfigurasi dapat berkembang menjadi kompromi skala besar (mis. pengambilalihan akun, pencurian data, atau penyalahgunaan infrastruktur). Oleh karena itu, pertahanan aplikasi *web* bukan sekadar fitur teknis tetapi bagian integral dari manajemen risiko organisasi yang melibatkan *developer, ops*, tim keamanan, dan kebijakan.

2. **Hubungan Siklus Serangan dan Pertahanan (*Attacker* Vs *Defender Mindset*)**

   Model "*attacker mindset*" mendorong *defender* untuk berpikir bagaimana seorang penyerang akan menemukan dan mengeksploitasi celah, misalnya dengan memanipulasi input, menguji otentikasi, atau mengandalkan *dependency* yang rentan. Pendekatan "*defender mindset*" menggabungkan *threat modeling*, mitigasi berlapis (*defense-in-depth*), otomatisasi keamanan (*scanning*, CI/CD *gating*), dan operasi insiden yang terstruktur. Menggabungkan kedua sudut pandang meningkatkan probabilitas menemukan masalah dini dan membangun kontrol yang efektif.

3. **Kerangka Standar Keamanan *Web*: OWASP Top 10, NIST CSF, ISO/IEC 27001**
   Dokumen seperti OWASP Top 10 menyediakan daftar risiko paling kritis terhadap aplikasi web dan pedoman mitigasinya; NIST CSF (termasuk versi 2.0) menawarkan kerangka manajemen risiko yang dapat diadaptasi organisasi; ISO/IEC 27001 lebih menekankan sistem manajemen keamanan informasi (ISMS) yang menyeluruh. Ketiganya sering dipakai bersamaan: OWASP untuk kontrol teknis aplikasi, NIST/ISO untuk pengelolaan risiko dan kebijakan.
4. **Studi Kasus Singkat: Contoh Serangan *Web* Dunia Nyata dan Dampaknya**
   Serangan *web* besar (mis. pencurian data akibat SQL *injection, skimming* kartu akibat XSS, atau gangguan layanan besar akibat konfigurasi yang salah) menunjukkan dampak finansial, reputasi, dan kepatuhan yang signifikan. Menelaah insiden nyata membuktikan: investasi pencegahan (*secure coding*, *patching,* WAF, *monitoring*) jauh lebih murah ketimbang biaya pemulihan dan litigasi setelah kompromi. (Sumber studi kasus per insiden dapat diambil dari laporan *vendor* keamanan dan publikasi insiden).

Jenis-Jenis Serangan *Web* dan Cara Kerjanya

1. **SQL *Injection***
   SQL *Injection* (SQLi) terjadi ketika aplikasi memasukkan *input* pengguna langsung ke *query database* tanpa parameterisasi, sehingga penyerang bisa menyisipkan potongan SQL untuk membaca, mengubah, atau menghapus data, dan kadang mengeksekusi perintah sistem pada *server database*.

   Dampaknya meliputi pencurian data pengguna, eskalasi hak akses, dan kompromi sistem *backend*. Pencegahan utama: *parameterized queries*/*prepared statements* dan penghapusan perilaku query dinamis.
2. ***Cross-Site Scripting* (XSS)**
   XSS memungkinkan penyerang menyuntikkan skrip *JavaScript* berbahaya ke halaman yang dilihat pengguna lain bentuknya dapat berupa *stored, reflected*, atau DOM-*based* XSS. Konsekuensinya

3. ***Backup* & *Disaster Recovery***
   Rencanakan *backup* terenkripsi, tes pemulihan (DR *drills*), dan pastikan *backup* tidak mudah diakses lewat jalur yang sama seperti sistem produksi untuk menghindari enkripsi/tebusan.
4. ***Security Awareness* & *Training* Rutin**
   Developer dan *ops* perlu pelatihan reguler tentang ancaman terbaru (mis. OWASP Top 10), praktik aman, serta simulasi *attack*/*response* untuk meningkatkan kesiapsiagaan organisasi.

Studi Kasus Implementasi Keamanan Web (Contoh Singkat)

1. **Contoh Pencegahan SQL *Injection* (Sebelum Vs Sesudah)**
   Sebelum: *query string* dibuat secara konkatenasi (rentan SQLi). Setelah: penggunaan *prepared statement*/ORM dengan *binding* parameter sehingga *input* tidak pernah diinterpretasikan sebagai kode SQL. Hasil: tidak ada *injection* dan operasi DB aman. (Lihat *cheat sheet* OWASP SQLi *Prevention* untuk contoh kode).
2. **Penerapan WAF Untuk Memblok DdoS**
   WAF disusun untuk *rate-limit* dan memblok pola permintaan mencurigakan; dipadukan dengan CDN untuk menyerap *traffic* besar. Setelah implementasi terjadi penurunan latensi dan penurunan kejadian *down time* saat serangan. (WAF perlu dikonfigurasi agar tidak mengganggu trafik sah).
3. ***Hardening* Konfigurasi *Login* dan *Session***
   Contoh: *set cookie HttpOnly; Secure; SameSite=Strict*, menambahkan MFA, membatasi percobaan *login*, dan memantau anomali akses mengurangi *account takeover*.

Daftar Pustaka

Anderson, Ross. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.

Bhuyan, Monowar, Dhruba Bhattacharyya, And Jugal Kalita. (2015). *Network Traffic Anomaly Detection and Prevention*. Springer.

Douligeris, Christos, and Aikaterini Serpanos. (2007). *Network Security: Current Status and Future Directions.* Wiley-IEEE.

Feiman, J., & Witty, R. (2012). *Web Application Firewall Magic Quadrant*. Gartner Research.

Fonseca, Jose, and Marco Vieira. (2008). *Mapping Software Faults With Web Security Vulnerabilities*. DSN 2008.

Grassi, Paul, Elaine Garcia, and James Fenton. (2017). NIST Digital Identity Guidelines. *NIST Special Publication 800-63*.

Halfond, William, Jeremy Viegas, and Alessandro Orso. (2006). A Classification of SQL Injection Attacks and Countermeasures. *IEEE Software Security Workshop.*

Holz, R., Amann, J., Mehani, O., Kaafar, M., & Ott, J. (2015). TLS In The Wild. *NDSS Symposium.*

Kent, Karen, et al. (2006). *Guide to Computer Security Log Management*. NIST.

Oppliger, Rolf. (2016). *SSL And TLS Theory and Practice*. Artech House.

OWASP Foundation. (2023). *OWASP Testing Guide 5.0*.

Ponemon Institute. (2022). *Cost of A Data Breach Report*. IBM Security.

Sandhu, R., et al. (1996). Role-Based Access Control Models. *IEEE Computer* 29(2).

Scarfone, Karen, and Peter Mell. (2009). *Guide to Enterprise Patch Management Technologies*. NIST Special Publication.

Sharma, Akhil, And Kailash Suryavanshi. (2015). Web Server Hardening. *International Journal of Computer Applications*.

Stuttard, Dafydd, and Marcus Pinto. (2011). *The Web Application Hacker's Handbook.* Wiley.

Verizon. (2023). *Data Breach Investigation Report*.

PROFIL PENULIS

Lilis Supratman, M.Si.

Lilis Supratman adalah seorang dosen dari lima bersaudara yang bertempat tinggal di Kota Bogor. Selama mengabdi di Universitas Pakuan Bogor sejak tahun 2007, menulis merupakan hobinya. Tidak kurang dari 9 buku bersertifikat ISBN yang sudah dirilis dan 13 *e-book* yang bersertifikat HaKI. Disiplin ilmu yang digeluti adalah mikrobiologi dengan cakupan materi jamur dan liken.

Aplikasi keilmuan diimplementasikan dalam bentuk kegiatan pengabdian masyarakat dalam berbagai topik yang bersifat multidisiplin (topik *stunting*, media *digital*, cerpen berbasis AI, pembuatan pupuk organik dan pembuatan lembar kerja/*worksheet*). Membaca adalah cara kita menyerap hikmah dari dunia, dan menulis adalah cara kita mengembalikan kebaikan itu kepada dunia. Saat kita membaca, kita memperluas pandangan dan menguatkan hati; saat kita menulis, kita meninggalkan jejak pemikiran agar orang lain ikut merasakan cahaya yang pernah menyinari kita. Tak perlu menjadi hebat dulu untuk mulai menulis, justru dengan menulis kita tumbuh, belajar, dan akhirnya memberi arti. Membaca dan menulis adalah pasangan serasi dalam memahami alam sekitar. Oleh karena itu, pahamilah bahwa "Cuplikan media sosial bisa menggiring persepsi. Tapi melalui buku, memberikan pemahaman yang utuh".

Email Penulis: lilis@unpak.ac.id.

BAB 8
RESPONS INSIDEN KEAMANAN

Dr. Eng. Ir. Abdul Wahid, S.T., M.Kom., IPM.
Universitas Negeri Makassar

Pendahuluan

Keamanan siber telah menjadi salah satu aspek paling kritis dalam dunia teknologi informasi saat ini. Pesatnya digitalisasi dan meningkatnya volume data yang disimpan secara digital telah melahirkan ancaman yang semakin kompleks dan beragam. Organisasi publik maupun swasta kerap menjadi sasaran serangan siber yang dapat merusak reputasi, menyebabkan kerugian finansial besar, hingga membahayakan data pribadi masyarakat.

Dalam menghadapi ancaman tersebut, respons insiden keamanan memegang peranan sangat vital. Kecepatan dan efektivitas respons menentukan seberapa besar dampak yang dapat diminimalkan (Nelson *et al.,* 2025). Respons yang lambat atau tidak terkoordinasi sering kali memperburuk situasi dan memperluas kerugian. Oleh karena itu, setiap organisasi wajib memiliki prosedur, tim, dan teknologi yang siap menangani insiden secara cepat dan sistematis.

Di tengah meningkatnya ancaman siber, respons insiden siber menjadi aspek vital yang diperlukan untuk memastikan keberlangsungan organisasi dan perlindungan terhadap aset informasi. Respons insiden bukan semata-mata masalah teknis; ia mencakup pengelolaan krisis, komunikasi yang efektif, dan pemulihan yang cepat setelah suatu insiden. Dalam konteks ini, pembentukan tim Tanggap Insiden Siber menjadi sangat penting.

Misalnya, badan pemerintah Indonesia, Badan Siber dan Sandi Negara (BSSN), telah merancang kebijakan untuk membentuk tim Tanggap Insiden Siber (CSIRT) yang kuat dan berkompeten di setiap instansi pemerintah, guna meningkatkan pertahanan keamanan siber nasional (Prabaswari *et al.,* 2022). Penelitian menunjukkan bahwa tim semacam ini bertanggung jawab untuk menangani insiden siber dengan baik, dan keputusan yang diambil di dalamnya sangat mempengaruhi efektivitas respon terhadap kejadian-kejadian tersebut (Dwiaji *et al.,* 2024).

Penanganan insiden yang efisien tidak hanya meminimalkan kerusakan, tetapi juga dapat memperkuat sistem pertahanan yang ada dan meningkatkan kepercayaan publik terhadap organisasi. Oleh karena itu, respons insiden keamanan harus dipahami sebagai bagian integral dari kebijakan keamanan siber yang lebih luas, yang tidak hanya berfokus pada pencegahan, tetapi juga pada kemampuan untuk

mengatasi insiden ketika terjadi (Sikder & Islam, 2023; Tanque & Foxwell, 2018).

Gambar 8.1: Lanskap Ancaman Siber

Sumber: Diolah Penulis.

Bab ini bertujuan memberikan panduan komprehensif mengenai respons insiden keamanan, mencakup identifikasi, penanggulangan, pemulihan, hingga pembelajaran pasca-insiden. Pembahasan juga mencakup peran tim respons insiden (CSIRT), alat dan teknologi terkini, kebijakan, komunikasi krisis, aspek hukum, serta tren masa depan respons insiden di era AI dan *cloud-native*.

Definisi dan Klasifikasi Insiden Keamanan

1. Definisi Insiden Keamanan

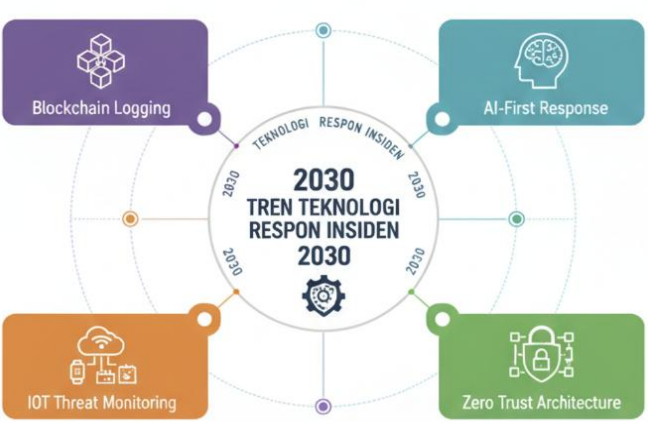
Insiden keamanan siber adalah setiap peristiwa yang mengganggu atau berpotensi mengganggu kerahasiaan, integritas, dan ketersediaan sistem informasi (ISO/IEC 27035-1, 2023). Insiden ini dapat muncul dalam berbagai bentuk, mulai dari percobaan akses tidak sah, gangguan layanan, hingga manipulasi data.

Dalam ranah keamanan siber, insiden seringkali melibatkan tindakan eksploitasi terhadap celah keamanan yang ada pada perangkat keras, perangkat lunak, maupun pada perilaku pengguna. Dengan kata lain, insiden keamanan adalah tanda bahwa suatu sistem telah menjadi target ancaman, baik yang bersifat disengaja maupun tidak disengaja.

b. Bagian dari manajemen risiko perusahaan
c. Keunggulan kompetitif, terutama bagi organisasi digital

Peran CISO dan tim keamanan akan semakin penting dalam struktur organisasi masa depan. Masa depan respons insiden dipengaruhi oleh kemajuan teknologi, kompleksitas ancaman, serta meningkatnya ketergantungan organisasi pada sistem *digital*.

Respons insiden tidak lagi sekadar menangani serangan setelah terjadi, tetapi menjadi kemampuan prediktif yang memanfaatkan AI, otomasi, *Zero Trust*, dan keamanan *cloud-native*. Organisasi yang mampu mengadopsi pendekatan ini akan memiliki ketahanan siber yang jauh lebih kuat dan siap menghadapi ancaman generasi berikutnya.



Gambar 8.5: Tren Teknologi Respons Insiden 2030
Sumber: Diolah Penulis.

Kesimpulan

Respons insiden keamanan merupakan komponen fundamental dalam pertahanan siber modern. Dalam era *digital* yang ditandai oleh kompleksitas sistem, ketergantungan tinggi pada teknologi, dan meningkatnya ancaman yang canggih, organisasi tidak dapat lagi mengandalkan pendekatan reaktif. Mereka harus mengembangkan kemampuan respons insiden yang terencana, terstruktur, dan adaptif terhadap dinamika ancaman siber yang terus berubah.

Bab ini telah menguraikan prinsip-prinsip penting yang menjadi dasar respons insiden yang efektif. Dimulai dari pemahaman mengenai definisi dan klasifikasi insiden keamanan, organisasi dipandu untuk mengenali berbagai jenis ancaman yang mungkin terjadi, mulai dari *malware*, pencurian data, hingga serangan terdistribusi dan kompromi rantai pasokan. Pemahaman ini menjadi prasyarat untuk menentukan strategi respons yang sesuai.

Fase-fase respons insiden identifikasi, penanggulangan, pemulihan, dan evaluasi membentuk kerangka kerja inti yang harus diintegrasikan dalam operasi keamanan sehari-hari. Setiap fase memerlukan perencanaan matang, koordinasi lintas tim, serta dokumentasi yang akurat untuk memastikan respons yang cepat dan terukur. Tim respons insiden memainkan peran sentral dalam siklus ini, dengan struktur peran yang jelas dan kolaborasi yang melibatkan pihak internal maupun eksternal.

Teknologi juga menjadi elemen yang tidak terpisahkan, dengan berbagai alat seperti SIEM, EDR, IDS/IPS, forensik digital, SOAR, hingga pendekatan *Zero Trust*. Kesemuanya berkontribusi pada peningkatan deteksi, mitigasi, dan pemulihan insiden. Namun, secanggih apa pun teknologi yang digunakan, respons insiden tidak akan optimal tanpa kebijakan, SOP, dan rencana respons yang kuat. Kebijakan ini memberikan arah, konsistensi, dan dasar hukum dalam menangani insiden.

Melalui analisis studi kasus mulai dari *WannaCry* hingga *SolarWinds* kita melihat bahwa banyak insiden besar berakar pada kelemahan prosedural, *human error*, keterlambatan *patching*, dan kurangnya koordinasi. Studi kasus ini memberikan pembelajaran penting bahwa respons insiden bukan hanya proses teknis, tetapi juga proses strategis dan komunikatif yang melibatkan transparansi, manajemen reputasi, dan kepatuhan regulasi.

Aspek hukum dalam respons insiden menunjukkan bahwa organisasi harus lebih berhati-hati dalam menjaga integritas data, melapor kepada regulator, mematuhi UU Perlindungan Data Pribadi, serta bekerja sama dengan aparat penegak hukum. Kegagalan memenuhi aspek hukum dapat membawa konsekuensi yang lebih berat dibanding insiden itu sendiri.

Memasuki masa depan, tantangan akan semakin kompleks. Serangan berbasis AI, eksploitasi IoT, keamanan *cloud-native*, hingga ancaman *supply chain* memerlukan pendekatan respons yang lebih adaptif dan prediktif. Ke depannya, respons insiden akan semakin bergeser dari model reaktif menuju model proaktif berbasis automasi dan kecerdasan buatan. Organisasi yang mampu berinvestasi dalam *Zero Trust*, SOAR, *threat intelligence*, serta pelatihan *human-centric* akan memiliki keunggulan signifikan dalam ketahanan siber.

Pada akhirnya, respons insiden bukan hanya soal memadamkan "kebakaran *digital*" ketika insiden terjadi. Lebih daripada itu, respons insiden adalah bagian dari strategi pertahanan berkelanjutan yang menggabungkan teknologi, kebijakan, manusia, dan budaya keamanan. Organisasi yang mengintegrasikan seluruh elemen ini tidak hanya akan lebih siap menghadapi ancaman, tetapi juga lebih mampu menjaga kepercayaan pelanggan, stabilitas operasional, dan keberlangsungan bisnis di era *digital*.

Daftar Pustaka

Abieba, O. A., Alozie, C. E., & Ajayi, O. O. (2025). Enhancing Disaster Recovery and Business Continuity in Cloud Environments Through Infrastructure As Code. *Journal of Engineering Research and Reports*, *27*(3), 127–136. https://doi.org/10.9734/jerr/2025/v27i31423.

Adawiyah, R., Prasetyo, M. A., Septiyan, R., Leonardy, S., & Calvin, M. (2022). Analysis of E-Commerce Data Breach And Theft. *Priviet Social Sciences Journal*, *2*(2), 11–14. https://doi.org/10.55942/pssj.v2i2.168.

Bamiatzi, V., Dowling, M., Gogolin, F., Kearney, F., & Vigne, S. (2023). Are The Good Spared? Corporate Social Responsibility As Insurance Against Cyber Security Incidents. *Risk Analysis*, *43*(12), 2503–2518. https://doi.org/10.1111/risa.14122.

Bayramova, A., Edwards, D. J., & Roberts, C. (2021). The Role of Blockchain Technology in Augmenting Supply Chain Resilience to Cybercrime. *Buildings*, *11*(7), 283. https://doi.org/10.3390/buildings11070283.

Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber Threats Classifications And Countermeasures in Banking and Financial Sector. *IEEE Access*, *11*, 125138–125158. https://doi.org/10.1109/ACCESS.2023.3327016

Dm, V. G., & Ananda, A. (2024). Kecerdasan Buatan untuk Security Orchestration, Automation And Response: Tinjauan Cakupan. *Jurnal Komputer Terapan*, *10*(1), 36–47. https://doi.org/10.35143/jkt.v10i1.6247.

Dwiaji, L., Widodo, A. M., Firmansyah, G., & Tjahyono, B. (2024). Analysis of Knowledge Management Strategies For Handling Cyber Attacks With The Computer Security Incident Response Team (CSIRT) In The Indonesian Aviation Sector. *Asian Journal of Social And Humanities*, *2*(6), 1341–1353. https://doi.org/10.59888/ajosh.v2i6.261.

Englbrecht, L., Langner, G., Pernul, G., & Quirchmayr, G. (2019). Enhancing Credibility of Digital Evidence Through Provenance-Based Incident Response Handling. *Proceedings of The 14th International Conference on Availability, Reliability and Security*, 1–6. https://doi.org/10.1145/3339252.3339275.

European Union Agency for Cybersecurity. (2023). ENISA Threat Landscape 2023: July 2022 to June 2023. *Publications Office*. https://data.europa.eu/doi/10.2824/782573.

González, F., Figueroa, A., López, C., & Aragón, C. (2019). Information Privacy Opinions on Twitter: A Cross-Language Study. *Companion Publication of The 2019 Conference on Computer Supported Cooperative Work and Social Computing*, 190–194. https://doi.org/10.1145/3311957.3359501.

Grispos, G., Glisson, W. B., & Storer, T. (2017). Enhancing Security Incident Response Follow-Up Efforts With Lightweight Agile Retrospectives. *Digital Investigation*, *22*, 62–73. https://doi.org/10.1016/j.diin.2017.07.006.

Gurulakshmanan, G., & Amarnath, R. N. (2024). Efficient And Robust Disaster Recovery System Using Cloud-Based Algorithms With Data Integrity. *Indonesian Journal of Electrical Engineering And Computer Science*, *35*(1), 388. https://doi.org/10.11591/ijeecs.v35.i1.pp388-396.

Hirai, H., Aoyama, T., Nyambayar, D., & Koshijima, I. (2017). *Framework For Cyber Incident Response Training*. 273–283. https://doi.org/10.2495/SAFE170251.

Hu, H., Zhang, L., Zhang, Z., Yao, X., & Wu, X. (2025). An Intelligent Playbook Recommendation Algorithm Based on Dynamic Interest Modeling For SOAR. *Symmetry*, *17*(11), 1851. https://doi.org/10.3390/sym17111851.

Ismail, A. (2024). Enhancing Cybersecurity Resilience Through Improved Technical Measures In Incident Response Strategies. *Wseas Transactions On Communications*, *23*, 76–81. https://doi.org/10.37394/23204.2024.23.10.

ISO/IEC 27035-1. (2023). *Information Technology Information Security Incident Management Part 1: Principles and Process*. ISO/IEC 2023. https://www.iso.org/standard/78973.html.

Jiménez, M. B., Fernández, D., Eduardo Rivadeneira, J., & Flores-Moyano, R. (2024). A Filtering Model for Evidence Gathering in an SDN-Oriented Digital Forensic and Incident Response Context. *IEEE Access*, *12*, 75792–75808. https://doi.org/10.1109/ACCESS.2024.3405588.

Jouini, M., & Rabai, L. B. A. (2014). Surveying and Analyzing Security Problems in Cloud Computing Environments. *Proceedings of the 2014 Tenth International Conference on Computational Intelligence and Security*, 689–693. https://doi.org/10.1109/CIS.2014.169

Lamb, C., & Zacchiroli, S. (2022). Reproducible Builds: Increasing the Integrity of Software Supply Chains. *IEEE Software*, *39*(2), 62–70. https://doi.org/10.1109/MS.2021.3073045.

Lapaire, J.-R. (2018). Why Content Matters. Zuckerberg, Vox Media And The Cambridge Analytica Data Leak. *ANTARES: Letras e Humanidades*, *10*(20), 88–110.

Martínez, J., & Durán, J. M. (2021). Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study. *International Journal of Safety And Security Engineering*, *11*(5), 537–545. https://doi.org/10.18280/ijsse.110505.

Muhrtala, T. O., & Ogundeji, M. (2013). Computerized Accounting Information Systems And Perceived Security Threats In Developing Economies: The Nigerian Case. *Universal Journal of Accounting and Finance*, *1*(1), 9–18. https://doi.org/10.13189/ujaf.2013.010102.

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident Response Recommendations And Considerations For Cybersecurity Risk Management: A CSF 2.0 community profile* (No. NIST SP 800-61r3; p. NIST SP 800-61r3). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-61r3.

Noman, H. A., & Abu-Sharkh, O. M. F. (2023). Code Injection Attacks in Wireless-Based Internet of Things (IoT): A Comprehensive Review And Practical Implementations. *Sensors*, *23*(13), 6067. https://doi.org/10.3390/s23136067.

Paul, B., & Rao, M. (2022). Zero-Trust Model For Smart Manufacturing Industry. *Applied Sciences*, *13*(1), 221. https://doi.org/10.3390/app13010221.

Prabaswari, Alfikri, M., & Ahmad, I. (2022). Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. *Matra Pembaruan: Jurnal Inovasi Kebijakan*, *6*(1), 1–14. https://doi.org/10.21787/mp.6.1.2022.1-14.

Prastowo, S. L., & Sudiana, D. (2024). Recommendations for a Framework for Handling Security Incidents of Electronic-Based Government Systems (SPBE) Using The ISO/IEC 27035: 2023 Standard. *JINAV: Journal of Information and Visualization*, *5*(1), 107–114. https://doi.org/10.35877/454RI.jinav2747.

Pretorius, M., & Ngejane, H. (2019). Best Practices for Establishment of a National Information Security Incident Management Capability (ISIMC). *The African Journal of Information and Communication (AJIC)*, *24*. https://doi.org/10.23962/10539/28656.

Regueiro, C., Seco, I., Gutiérrez-Agüero, I., Urquizu, B., & Mansell, J. (2021). A Blockchain-Based Audit Trail Mechanism: Design And Implementation. *Algorithms*, *14*(12), 341. https://doi.org/10.3390/a14120341.

Rizvi, S., Scanlon, M., Mcgibney, J., & Sheppard, J. (2022). Application of Artificial Intelligence to Network Forensics: Survey, Challenges And Future Directions. *IEEE Access*, *10*, 110362–110384. https://doi.org/10.1109/ACCESS.2022.3214506.

Sajan, D. P. P. (2024). A Comprehensive Analysis of WannaCry Ransomware. *International Journal of Scientific Research In Engineering And Management*, *08*(008), 1–5. https://doi.org/10.55041/IJSREM37242.

Schlette, D., Caselli, M., & Pernul, G. (2021). A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. *IEEE Communications Surveys & Tutorials*, *23*(4), 2525–2556. https://doi.org/10.1109/COMST.2021.3117338.

Shutock, M., & Dietrich, G. (2022). *Security Operations Centers: A Holistic View on Problems and Solutions*. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2022.907.

Sikder, A. S., & Islam, Md. R. (2023). Enhancing Cyber-Resilience Within Bangladesh's Legal Framework: Evaluating Preparedness And Mitigation Strategies Against Technologically-Driven Threats: Enhancing Cyber-Resilience Within Bangladesh's Legal Framework. *International Journal of Imminent Science & Technology.*, *1*(1), 40–57. https://doi.org/10.70774/ijist.v1i1.6.

Tanque, M., & Foxwell, H. J. (2018). Cyber Resilience For The Internet of Things. In *Handbook of Research on Information And Cyber Security In The Fourth Industrial Revolution* (pp. 304–335). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-5225-4763-1.ch011.

Trajanovski, T., & Zhang, N. (2021). An Automated and Comprehensive Framework For IoT Botnet Detection And Analysis (IoT-BDA). *IEEE Access*, *9*, 124360–124383. https://doi.org/10.1109/ACCESS.2021.3110188.

Tsuchiya, A., Fraile, F., Koshijima, I., Ortiz, A., & Poler, R. (2018). Software Defined Networking Firewall For Industry 4.0 Manufacturing Systems. *Journal of Industrial Engineering and Management*, *11*(2), 318. https://doi.org/10.3926/jiem.2534.

Van Der Kleij, R., Kleinhuis, G., & Young, H. (2017). Computer Security Incident Response Team Effectiveness: A Needs Assessment. *Frontiers in Psychology*, *8*, 2179. https://doi.org/10.3389/fpsyg.2017.02179.

PROFIL PENULIS

Dr. Eng. Ir. Abdul Wahid, S.T., M.Kom., IPM.

Penulis merupakan Dosen Teknik Komputer UNM lulusan Program *Doctoral Kanazawa University*, Jepang dengan Kapakaran pada bidang *Information Security* dan Kriptografi. Beberapa Artikel ilmiah bidang *computer security* telah dipublikasikan dan salah satu diantaranya yang berjudul "*Toward Constructing a Secure Online Examination Systems*" mendapatkan *Best Presentation Award* pada A3 *Foresight Program Annual Workshop Research on Next Generation Networks and Network Security* tanggal 14-15 Juli 2014 di Gyeongju, Korea Selatan.

Penulis juga memiliki kemampuan sebagai senior *web developer* dan *security specialist* dengan beberapa pengalaman dan sertifikasi Internasional bidang keamanan. Penulis adalah seorang peneliti dan dosen pada mata kuliah Keamanan Komputer, Keamanan *Website, Penetration Testing*, Kriptografi dan *Digital* Forensik. Beberapa keterampilan yang dimiliki Adalah mahir dalam beberapa Bahasa pemrograman termasuk HTML, PHP, *Javascript*, CSS, C++ dan MySQL. Memiliki pengalaman dalam *Leadership, Project Management* dan *Customer Relations*.

Email Penulis: wahid@unm.ac.id.

HACKER VS DEFENDER

Panduan Komprehensif dari Serangan hingga Pertahanan Siber

Dalam era digital yang terus melesat, dunia siber telah menjadi medan pertempuran baru yang tak kasat mata. Di satu sisi, ancaman siber terus berevolusi dengan kecepatan yang mengkhawatirkan, mulai dari eksploitasi sederhana hingga serangan canggih yang didanai negara. Di sisi lain, para profesional keamanan siber dituntut untuk selalu sigap, waspada, dan terus belajar untuk membangun pertahanan yang tangguh. Buku ini hadir untuk menjembatani kedua dunia tersebut, membahas taktik, teknik, dan prosedur dari kedua perspektif baik dari sudut pandang penyerang (*hacker*) maupun pembela (*defender*). Tujuan utama penulisan buku ini bukan untuk mengajarkan kejahatan, melainkan untuk memberikan pemahaman yang mendalam dan holistik. Dengan memahami bagaimana sebuah serangan dilancarkan, kita akan mampu merancang dan mengimplementasikan strategi pertahanan yang jauh lebih efektif dan proaktif. “Untuk mengalahkan musuh, Anda harus mengenal musuh Anda.” Prinsip inilah yang menjadi fondasi setiap bab dalam buku ini, sebagai berikut: (1) Dunia Hacker dan Defender; (2) Konsep Dasar IT *Security*; (3) Jenis-Jenis Ancaman Siber; (4) *Scanning* & *Enumeration*; (5) *Persistence* Dan *Backdoor*; (6) *Hardening* Sistem Operasi Dan Aplikasi; (7) Mencegah Dan Menangkal Serangan Web; dan (8) Respons Insiden Keamanan

sada kurnia pustaka

ISBN 978-634-7522-03-0
9 786347 522030