Konsep Ancaman dan Strategi Pertahanan Siber Berbasis Ethical Hacking

Penulis :
Dewa Nicholas Aryodha
Hendro Wijayanto

Penerbit
REDTECH PUTRA BENUA

Konsep Ancaman dan Strategi Pertahanan Siber Berbasis Ethical Hacking

Penulis:
Dewa Nicholas Aryodha
Hendro Wijayanto

Desain Cover:
Hendro Wijayanto

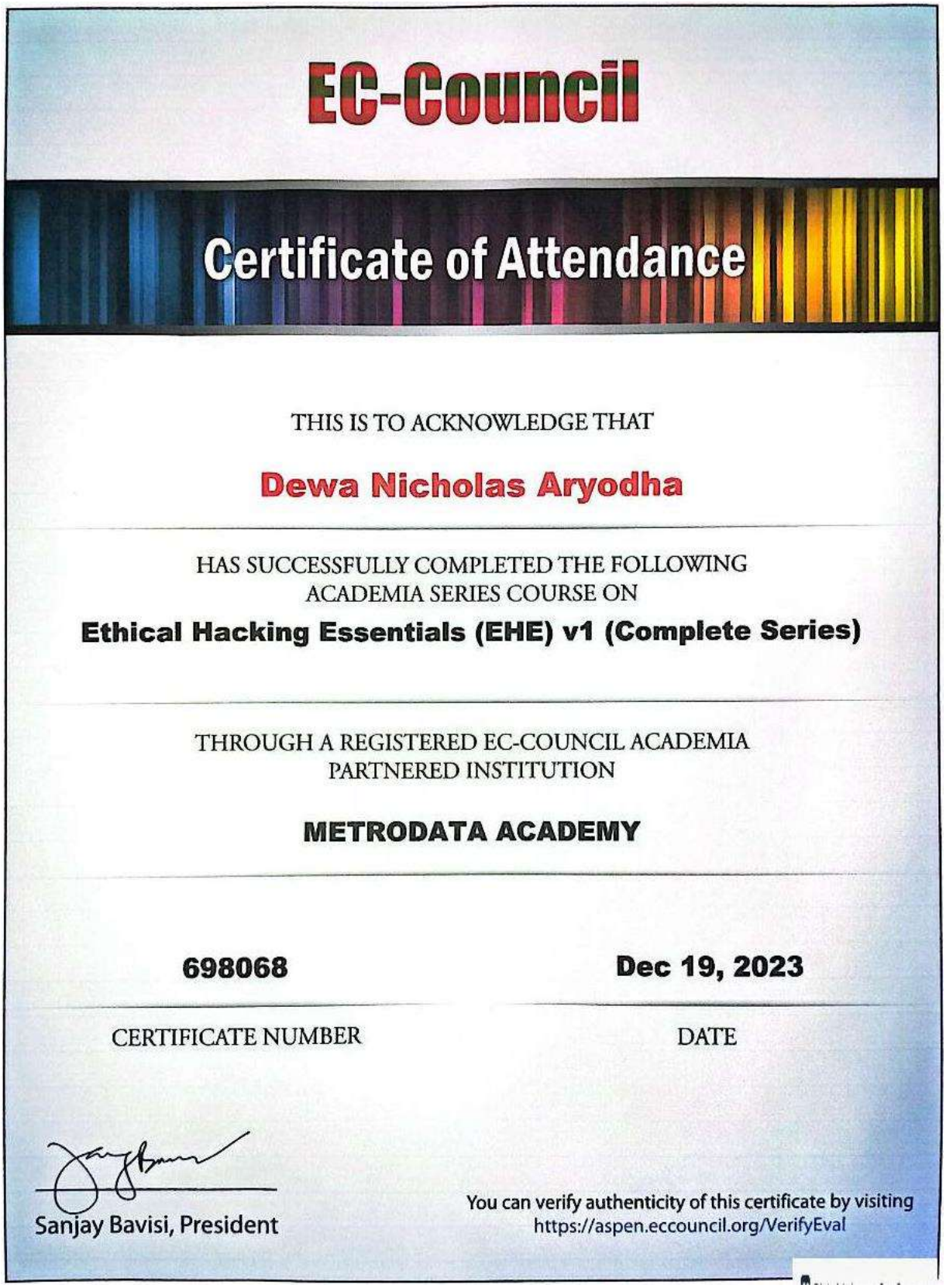
Tata Letak:
Perpustakaan Universitas Tiga Serangkai

Proofreader:
Perpustakaan Universitas Tiga Serangkai

ISBN:
978-634-04-1696-1

Cetakan Pertama:
Juli 2025

Buku ini diterbitkan atas kerjasama antara Perpustakaan Universitas Tiga Serangkai (Kampus Terpadu Gedung A Lantai 3 Jln. KH. Samanhudi No. 84-86 Surakarta) dan Redtech Putra Benua. Penerbitan buku ini merupakan hasil kerja sama dalam rangka pengembangan literasi akademik dan peningkatan kualitas sumber daya manusia di lingkungan perguruan tinggi. Naskah disusun oleh mahasiswa, tenaga kependidikan atau dosen dari Universitas Tiga Serangkai dan difasilitasi oleh Penerbit Redtech Putra Benua dalam proses editing, layout, dan distribusi nasional.


EC-Council
Certificate of Attendance
THIS IS TO ACKNOWLEDGE THAT
Dewa Nicholas Aryodha
HAS SUCCESSFULLY COMPLETED THE FOLLOWING
ACADEMIA SERIES COURSE ON
Ethical Hacking Essentials (EHE) v1 (Complete Series)
THROUGH A REGISTERED EC-COUNCIL ACADEMIA
PARTNERED INSTITUTION
METRODATA ACADEMY
698068
Dec 19, 2023
CERTIFICATE NUMBER
DATE
Sanjay Bavisi, President
You can verify authenticity of this certificate by visiting
https://aspen.eccouncil.org/VerifyEval

KATA PENGANTAR PENULIS

Bismillahirrahmanirrahim,

Segala puji dan syukur kehadirat Allah Subhana Wata'ala yang telah melimpahkan rahmat, taufiq, hidayah, dan inayah kepada hambanya, Shalawat serta salam selalu terlimpahkan pada Nabi Muhammad Shallallahu'alaihi wassalam. Saya sebagai penulis ingin mengucapkan rasa syukur atas nikmat yang telah diberikan sehingga karya tulis Buku ini dapat terselesaikan dengan baik.

Di era digital yang semakin kompleks dan terhubung, keamanan informasi telah menjadi kebutuhan fundamental, bukan sekadar opsi tambahan. Ancaman siber dapat menyerang siapa saja baik individu, organisasi, maupun institusi pemerintah dan dampaknya bisa sangat merugikan. Oleh karena itu, memahami konsep ethical hacking dan strategi pertahanan menjadi kunci penting untuk membangun sistem yang tangguh terhadap berbagai bentuk serangan digital.

Buku ini hadir sebagai panduan komprehensif yang membahas berbagai aspek fundamental dalam dunia ethical hacking dan keamanan siber. Materi disusun secara sistematis mulai dari pengenalan konsep ethical hacking, klasifikasi hacker, jenis-jenis ancaman, teknik eksploitasi, hingga metode pertahanan dan proses penetration testing. Tidak hanya teori, buku ini juga menyoroti elemen-elemen praktis seperti taktik, teknik, dan prosedur (TTPs), indikator kompromi (IoCs), serta langkah-langkah pemetaan kerentanan dan respon insiden.

Sebagian pendekatan dan struktur visual dalam buku ini merupakan hasil pengembangan mandiri yang terinspirasi dari referensi materi *Ethical Hacking Essentials* terbitan EC-Council sebuah institusi global yang telah lama dikenal dalam pengembangan sertifikasi dan pendidikan di bidang keamanan siber. Namun demikian, seluruh konten dalam buku ini disesuaikan dengan pendekatan edukatif yang lebih terbuka, naratif, dan kontekstual agar mudah dicerna oleh pembaca dari berbagai latar belakang.

Ucapan terima kasih saya sampaikan kepada semua pihak yang telah memberikan dukungan, masukan, dan inspirasi selama proses penyusunan buku ini. Semoga karya ini dapat memberikan kontribusi positif dalam

meningkatkan literasi keamanan siber dan menjadi bekal awal yang berharga bagi siapa pun yang ingin terjun lebih dalam ke dunia ethical hacking.

Saya menyadari bahwa dalam penyusunan buku ini masih terdapat berbagai kekurangan, baik dari segi isi, penyampaian, maupun teknis penulisan. Untuk itu, saya sangat terbuka terhadap kritik dan saran demi perbaikan di edisi-edisi berikutnya. Semoga buku ini dapat bermanfaat dan menjadi pijakan awal menuju pemahaman yang lebih dalam tentang pentingnya pertahanan siber di era digital.

Surakarta, 7 Juli 2024

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
Konsep Ethical Hacking

Tujuan Bab

Bab ini disusun untuk membekali pembaca dengan pemahaman menyeluruh tentang dunia ethical hacking dan keamanan siber. Di dalamnya, pembaca akan diajak untuk memahami bagaimana metodologi Cyber Kill Chain digunakan dalam menganalisis setiap tahap serangan siber secara sistematis. Selain itu, modul ini juga mengupas secara mendalam konsep Taktik, Teknik, dan Prosedur (TTPs) yang biasa diterapkan oleh para peretas dalam beragam skenario nyata.

Sebagai bagian dari deteksi dan pencegahan serangan, pembaca juga akan dikenalkan pada berbagai jenis Indikator Kompromi (IoCs), yaitu tanda-tanda awal yang dapat menunjukkan adanya ancaman di dalam sistem. Modul ini tidak hanya berhenti pada aspek teknis, tetapi juga memperkenalkan konsep dasar peretasan, termasuk klasifikasi hacker berdasarkan motivasi serta pendekatan yang mereka gunakan dalam mengeksekusi serangan.

Untuk melengkapi pemahaman tersebut, materi ini juga memandu pembaca menyusuri setiap fase dalam siklus peretasan, mulai dari proses rekognisi hingga ke tahap eksploitasi. Di akhir, pembaca akan diajak mengenal secara utuh apa itu Ethical Hacking, termasuk peran dan ruang lingkupnya dalam konteks pertahanan siber, serta meninjau berbagai tools yang biasa digunakan oleh para ethical hacker untuk menguji dan memperkuat sistem keamanan.

Latar Belakang

Di era digital yang terus berkembang, salah satu ancaman terbesar bagi bisnis adalah kejahatan siber. Ekosistem e-commerce yang semakin maju telah memperkenalkan berbagai teknologi baru, termasuk lingkungan komputasi berbasis cloud. Serangkaian pelanggaran keamanan dalam beberapa tahun

terakhir telah membuat banyak organisasi menyadari pentingnya sistem keamanan informasi yang efektif.

Ethical hacking memungkinkan organisasi untuk mengevaluasi keamanan sistem mereka secara objektif. Saat ini, peran seorang ethical hacker semakin penting, karena mereka secara aktif menguji dan mengidentifikasi celah keamanan dalam infrastruktur teknologi untuk memperbaiki kelemahan yang ada.

Modul ini dimulai dengan pengenalan tentang metodologi Cyber Kill Chain dan indikator kompromi (IoCs). Selain itu, modul ini memberikan wawasan tentang konsep peretasan dan berbagai jenis hacker. Selanjutnya, modul ini juga membahas tahapan dalam siklus peretasan dan diakhiri dengan diskusi mengenai konsep ethical hacking, ruang lingkupnya, serta batasannya.

1.1 Metodologi Cyber Kill Chain

Cyber Kill Chain merupakan pendekatan yang bersifat sistematis digunakan untuk memahami bagaimana sebuah serangan siber dapat dilakukan terhadap suatu organisasi. Model ini membantu organisasi mengenali berbagai ancaman potensial di setiap tahap serangan serta langkah-langkah yang dapat diterapkan untuk mengatasinya.

Selain itu, dengan cara ini diharapkan dapat memberikan wawasan yang lebih mendalam bagi para profesional keamanan dalam menganalisis strategi yang digunakan oleh penyerang. Dengan pemahaman ini, organisasi atau perusahaan dapat menerapkan berbagai kontrol keamanan yang sesuai untuk melindungi infrastruktur teknologi informasi mereka.

Bagian ini akan membahas konsep pada Cyber Kill Chain, pola umum yang digunakan oleh peretas dalam melakukan serangan Tactic, Technique, and Procedure (TTP), cara mengenali dan mengidentifikasi perilaku penyerang, serta indikator yang menunjukkan adanya pelanggaran keamanan (IoCs).