

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

Hak Cipta 2025, Pada Penulis

Hak Cipta Dilindungi Oleh Undang-Undang

Copyright © 2025 pada Penerbit Redtech Putra Benua

All Right Reserved

Dilarang keras menerjemahkan, memfotokopi, atau memperbanyak sebagian atau seluruh isi buku ini tanpa izin tertulis dari Penulis dan Penerbit.

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

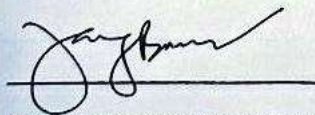
METRODATA ACADEMY

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 kehadiran 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

BAB I Konsep Ethical Hacking	1
Tujuan Bab	1
Latar Belakang	1
1.1 Metodologi Cyber Kill Chain	2
1.1.1 Definisi dan Tahapan Metodologi Cyber Kill Chain	3
1.1.2 Taktik, Teknik, dan Prosedur (TTPs)	22
1.1.3 Identifikasi Sifat Penyerang (Adversary Behavioral Identification)	25
1.1.4 Indikator Kompromi (IoCs)	30
1.1.5 Jenis Jenis Kategori dalam Indikator Kompromi	32
1.2 Konsep dan Jenis Hacking	35
1.2.1 Pengertian Hacking	35
1.2.2 Orang orang yang disebut Hacker	36
1.2.3 Kategori Hacker Berdasarkan Kelasnya	37
1.3 Tahapan-Tahapan dalam Proses Peretasan	44
1.3.1. Tahap Peretasan: Pengintaian (Reconnaissance)	45
1.3.2. Scanning	47
1.3.3. Gaining Acces	53
1.3.4. Maintaining Acces	56
1.3.5. Clearing Track	57
1.4. Konsep, Ruang Lingkup, dan Batasan Ethical Hacking	60
1.4.1. Mengapa memerlukan Ethical Hacking	62
1.4.2. Ruang Lingkup dan Keterbatasan Ethical Hacking	65
1.4.3 Keterampilan yang diperlukan Ethical Hacker	68

1.5. Alat atau Tools yang digunakan dalam Ethical Hacking	70
1.5.1. Pengumpulan Informasi Awal Menggunakan Teknik Google Hacking.....	70
1.5.2 Reconnaissance Tools	73
Kesimpulan.....	81
BAB II Ancaman Keamanan dan Penilaian Kerentanan Informasi.....	83
Latar Belakang	83
Tujuan Bab	84
2.1 Definisi Ancaman dan Sumber dari Ancaman	85
2.1.1 Definisi Ancaman	86
2.1.2 Threat Resource (Sumber Ancaman)	89
2.2 Malware dan Jenis Malware	92
2.2.1 Definisi Malware	93
2.2.2 Tujuan Hacker Menggunakan Malware	93
2.2.3 Bagaimana Malware dapat Menginfeksi atau Masuk ke System ..	95
2.2.4 Teknik Umum yang Digunakan Penyerang untuk Menyebarkan Malware di Web.....	102
2.2.5 Komponen Utama Malware.....	105
2.2.6 Jenis Jenis Malware dan Strategi Pertahanannya.....	108
2.3. Kerentanan (Vulnerability).....	201
2.3.1 Definisi Kerentanan.....	201
2.3.2 Klasifikasi Jenis Kerentanan	205
2.3.3 Beberapa Contoh Kerentanan pada Sistem Keamanan Jaringan ..	209
2.3.4 Dampak yang di akibatkan oleh Kerentanan	212
2.4. Penilaian Kerentanan (Vulnerability Assesment)	214
2.4.1 Definisi Penilaian dalam sebuah Kerentanan (Vulnerability Assesment)	215

2.4.2 Identifikasi Kerentanan dan Sumber Daya	217
2.4.3 Vulnerability Scanning Approaches	223
2.4.4 Jenis Jenis Penilaian Kerentanan	228
2.4.5 Siklus Manajemen Kerentanan	236
2.4.6 Alat Alat (Tools) untuk melakukan Penilaian Kerentanan	239
2.4.7 Eksploitasi Kerentanan	244
Kesimpulan.....	249
BAB III Teknik Teknik Peretasan dan Strategi Pertahanan (Countermeasure)	251
Latar Belakang	251
Tujuan	252
3.1 Teknik Rekayasa Sosial dan Strategi Pertahanan (Social Engineering)	253
3.1.1 Konsep Rekayasa Sosial dan Fasenya.....	254
3.1.1.1 Definisi tentang Serangan Rekayasa Sosial	256
3.1.1.2 Target Umum dari Rekayasa Sosial	257
3.1.1.3 Dampak Serangan Rekayasa Sosial terhadap Organisasi atau Perusahaan	259
3.1.1.4 Perilaku yang Rentan terhadap Serangan Rekayasa Sosial.....	260
3.1.1.5 Beberapa Faktor penyebab Organisasi atau Perusahaan Rentan Serangan Rekayasa Sosial	262
3.1.1.6 Penyebab Serangan Sosial berdampak Efektif.....	264
3.1.1.7 Fase Fase umum dalam Serangan Rekayasa Sosial.....	266
3.1.2 Teknik Teknik Rekayasa Sosial	268
3.1.2.1 Jenis Jenis Rekayasa Sosial.....	269
3.1.2.1.1 Rekayasa Berbasis Manusia (Human Based Social Engineering.....	275

3.1.2.1.2 Rekayasa Sosial Berbasis Komputer (Computer Base Social Engineering)	279
3.1.2.1.3 Rekayasa Sosial Berbasis Mobile (Mobile Based Social Engineering)	288
3.1.2.2 Ancaman dari Orang Dalam & Pencurian Identitas (Insider Threats and Identity Theft)	290
3.1.2.2.1 Ancaman dan Serangan Orang Dalam	291
3.1.2.2.2 Penyebab terjadinya Serangan Orang Dalam	294
3.1.2.2.3 Jenis Jenis Ancaman dari Dalam	295
3.1.2.2.4 Mengapa Serangan Orang Dalam Sangat Efektif	297
3.1.2.2.5 Pencurian Identitas (Identity Theft)	299
3.1.3 Strategi Pertahanan (Countermeasure) dari Serangan Rekayasa Sosial	301
3.1.3.1 Pertahanan Serangan Rekayasa Sosial (Sosial Engineering Countermeasure)	301
3.1.3.2 Strategi Pertahanan Ancaman Orang Dalam (Insider Threats Countermeasure)	304
3.1.3.3 Strategi Pertahanan terhadap Pencurian Identitas (Identity Theft Countermeasure)	306
3.1.3.4 Cara Mendeteksi Email yang mengganggu Phising	309
3.1.3.5 Anti-Phising Toolbar	311
3.1.3.6 Alat (Tools) Rekayasa Sosial	313
3.1.3.7 Audit Keamanan Organisasi Serangan Phising dengan OhPhish	315
3.2 Teknik Peretasan Kata Sandi dan Strategi Pertahanan (Password Cracking and Countermeasure)	316
3.2.1 Teknik-teknik Peretasan Kata Sandi	318
3.2.1.1 Password Cracking	318

3.2.1.2 Password Complexity (Kompleksitas Kata Sandi)	319
3.2.1.3 Microsoft Authentication.....	321
3.2.1.4 Jenis Serangan Terhadap Password	324
3.2.1.5 Teknik Peretasan Password Menggunakan Dictionary, Brute-Force, dan Rule-Based Attack.....	327
3.2.1.6 Password Guessing.....	330
3.2.1.7 Default Password	332
3.2.1.8 Teknik Peretasan Kata Sandi dengan Menggunakan Malware	333
3.2.1.9 Teknik Peretasan Kata Sandi dengan Man-in-the-Middle (MITM) dan Replay Attack.....	335
3.2.1.10 Rainbow Table Attack	338
3.2.2 Kasus Password Cracking di Indonesia	340
3.2.2.1 Kasus Tokopedia (2020) – Hash Password Bocor, Jadi Target Rainbow Table.....	340
3.2.2.2 Kasus Cermati.com (2020) – Password Bcrypt Bisa Aman, Tapi Data Lain Bikin Gampang Ditebak.....	340
3.2.2.3 Kasus BRI Life (2021) – Bocor Lewat Akses Internal, Jadi Jalan Buat Keylogger dan Cracking.....	341
3.2.2.4 Kasus BPJS Kesehatan (2021) – Dugaan Akses Lewat Sistem Lawas dan Password Default.....	341
3.2.2.5 Kasus Pemilu – Peretasan Situs KPU oleh Dani Firmansyah (2004)	342
3.2.2.6 Kasus MyIndiHome (2023) – Gabungan Password Reuse dan Credential Stuffing.....	343
3.2.3 Alat (Tools) Peretasan Kata Sandi.....	343
3.2.4 Strategi Pertahanan dari Serangan Peretasan Kata Sandi	345
KESIMPULAN	350

Password Cracking & Technique	350
3.3 Serangan Server Website & Aplikasi Website dan Strategi Penanggulangannya.....	351
3.3.1 Web Server	352
3.3.1.1 Pengenalan Web Server	353
3.3.1.1.1 Komponen Utama dalam Web Server (Web Server Components).....	356
3.3.1.1.2 Masalah Keamanan Web Server	358
3.3.1.1.3 Dampak Serangan terhadap Web Server	362
3.3.1.1.4 Penyebab Web Server terkena Hacking	364
3.3.1.2 Berbagai Jenis Serangan pada Web Server	367
3.3.1.2.1 DNS Server Hijacking.....	367
3.3.1.2.2 Serangan Direktor Traversal.....	369
3.3.1.2.3 Web Defacement.....	371
3.3.1.2.4 Miskonfigurasi Server Web.....	373
3.3.1.2.5 Serangan SSH Brute Force.....	374
3.3.1.2.6 Serangan Web Server menggunakan Metode Password Cracking.....	378
3.3.1.2.7 Serangan Web Server menggunakan Metode Server-Side Request Forgery (SSRF)	382
3.3.1.3 Beberapa Tools atau Alat yang digunakan untuk Menyerang Server Web.....	386
3.3.1.3.1 Metasploit Framework.....	387
3.3.1.3.2 Tools atau alat Lain untuk Menyerang Web Server	388
3.3.1.4 Strategi Pertahanan Serangan Web Server (Countermeasure)	389
3.3.1.4.1 Strategi Pertahanan dari Serangan Web Server	389

3.3.1.4.2 Tools Keamanan untuk Serangan Web Server	395
3.3.2 Website Aplikasi.....	398
3.3.2.1 Memahami Arsitektur Aplikasi Website dan Lapisan Keretannya.....	398
3.3.2.1.1 Memahami Cara Kerja Aplikasi Web	401
3.3.2.1.2 Arsitektur Aplikasi Web	405
3.3.2.1.3 Web Services	408
3.3.2.1.4 Jenis-jenis Web Service.....	413
3.3.2.1.5 Lapisan Kerentanan Sistem (Vulnerability Stack).....	416
3.3.2.2 Membahas Ancaman dan Serangan terhadap Aplikasi Web	420
3.3.2.3 Strategi Pertahanan Terhadap Serangan Aplikasi Web	448
3.3.3 Serangan SQL Injection	453
3.3.3.1 Definisi, Jenis Jenis Serangan, dan Tools SQL Injection.....	454
3.3.3.1.1 Definisi SQL Injection	454
3.3.3.1.2 Hal yang Harus di perhatikan SQL Injection	455
3.3.3.1.3 Teknologi Server Side di SQL Injection.....	456
3.3.3.1.4 Jenis Jenis SQL Injection	457
3.3.3.1.5 In-Band SQL Injection.....	458
3.3.3.1.6 Error Based SQL Injection	459
3.3.3.1.7 Out-of-Band SQL Injection.....	461
3.3.3.1.8 Blind SQL Injection tipe Boolean Exploitation (Inferential SQL Injection)	462
3.3.3.1.9 Blind SQL Injection tipe Heavy Query	463
3.3.3.1.10 Tools yang digunakan dalam Serangan SQL Injection.....	463
3.3.3.2 Strategi Pertahanan Serangan SQL Injection	466
KESIMPULAN	473

Web Application Attack & Countermeasure	473
3.4 Serangan pada Level Jaringan dan Strategi Pertahanan.....	475
Latar Belakang.....	476
Tujuan Modul.....	476
3.4.1 Penyadapan pada Jaringan (Sniffing)	477
3.4.1.1 Memahami Konsep Packet Sniffing.....	479
3.4.1.1.1 Definisi Packet Sniffing	480
3.4.1.1.2 Bagaimana Sniffing bisa Bekerja	483
3.4.1.1.3 Jenis Jenis Sniffing	487
3.4.1.1.4 Cara Hacker Meretas Jaringan menggunkan Sniffing .	493
3.4.1.1.5 Protokol yang Rentan terhadap Sniffing	495
3.4.1.2 Membahas Teknik Sniffing.....	498
3.4.1.2.1 MAC Flooding	499
3.4.1.2.2 Serangan Kekosongan DHCP (DHCP Starvation Attack)	501
3.4.1.2.3 Serangan Pemalsuan ARP (ARP Spoofing Attack)	505
3.4.1.2.4 Pemalsuan atau Duplikasi Alamat MAC.....	510
3.4.1.2.5 DNS Poisoning.....	513
3.4.1.2.6 Tools atau Alat yang digunakan dalam Serangan Metode Sniffing.....	517
3.4.1.3 Membahas Strategi Pertahanan Sniffing.....	519
3.4.2 Denial Of Service	524
3.4.2.1 Definisi, Jenis-Jenis Serangan DoS dan DDoS, dan tools yang digunakan	524
3.4.2.1.1 Pengertian DoS (Denial of Service)	524
3.4.2.1.2 Pengertian DDoS (Distributed Denial of Service)	526
3.4.2.1.3 Teknik Teknik Serangan DoS atau DDoS	532

3.4.2.1.4 Tools atau Alat untuk Serangan DoS/DDoS.....	545
3.4.2.2 Membahas Strategi Pertahanan terhadap Serangan DoS dan DDoS.....	550
3.4.2.2.1 Strategi Pertahanan Serangan DoS & DDoS	551
3.4.2.2.2 Alat-alat (Tools) untuk Melindungi Serangan DoS & DDoS	554
3.4.3 Pembajakan Sesi (Session Hijacking)	557
3.4.3.1 Membahas Definisi, Jenis-Jenis, dan Tools atau alat Serangan Pembajakan Sesi	558
3.4.3.1.1 Definisi dari Sesi Pembajakan.....	558
3.4.3.1.2 Faktor Keberhasilan Pembajakan Sesi.....	560
3.4.3.1.3 Proses dari Pembajakan Sesi.....	563
3.4.3.1.4 Jenis Jenis Pembajakan Sesi.....	565
3.4.3.1.5 Pembajakan Sesi dengan Mode OSI.....	567
3.4.3.1.6 Perbedaan Teknik Hijacking dan Spoofing	569
3.4.3.1.7 Alat alat (Tools) untuk Serangan Sesi Pembajakan.....	573
3.4.3.2 Membahas Strategi Pertahanan terhadap Pembajakan Sesi	577
3.4.3.2.1 Metode untuk Mendeteksi Pembajakan Sesi.....	578
3.4.3.2.2 Strategi Pertahanan Pembajakan Sesi.....	580
3.4.3.2.3 Alat atau Tools yang digunakan untuk Mendeteksi Pembajakan Sesi	583
Kesimpulan	587
Serangan pada Level Jaringan dan Strategi Pertahanan	587
BAB IV Penetration Testing – Pemahaman, Metodologi, dan Strategi.....	588
Latar Belakang	588
Tujuan	589

4.1 Pengertian dan Manfaat Penetration Testing.....	589
4.1.1 Definisi Penetration Testing	590
4.1.2 Manfaat Penetration Testing Secara Mendalam	591
4.1.3 Perbandingan dari Audit Keamanan, Evaluasi Kerentanan, dan Penetration Test.....	595
4.2 Strategi, Proses, Fase, dan Metodologi Penetration Testing.....	599
4.2.1 Strategi Penetration Testing.....	600
4.2.2 Proses Penetration Testing	602
4.2.3 Fase-fase Serangan dalam Penetration Testing	605
4.2.4 Metodologi untuk Pengujian Penetration Testing	609
4.3 Panduan dan Rekomendasi untuk Penetration Testing	612
4.3.1 Karakteristik dari Penetration Testing yang baik.....	612
4.3.2 Momen Penetration Testing	614
4.3.3 Etika Penetration Tester.....	616
4.3.4 Cara seorang Pentester untuk Berkembang.....	617
4.3.5 Profil yang baik sebagai Penetration Tester.....	620
4.3.6 Tanggung Jawab Sebagai Seorang Pentester	622
4.3.7 Jenis Resiko yang terkait dengan Penetration Testing	625
4.3.8 Kualifikasi, Pengalaman, Sertifikasi, dan Keterampilan yang Dibutuhkan untuk Seorang Penetration Tester	627
Kesimpulan.....	632

DAFTAR GAMBAR

Gambar 1 Metodologi Cyber Kill Chain.....	3
Gambar 2 Skema Serangan Trojans	113
Gambar 3 Skema Penyebaran Worms	154
Gambar 4 Skema Keylogger	167
Gambar 5 Skema Penyerangan Botnets.....	173
Gambar 6 Qualys VM	241
Gambar 7 Opening Rekayasa Sosial	253
Gambar 8 Publish Aplikasi Berbahaya.....	273
Gambar 9 Skema Replikasi Apk Resmi.....	274
Gambar 10 Skema Aplikasi Keamanan Palsu	275
Gambar 11 Jenis Jenis Phising	283
Gambar 12 Opening Teknik Peretasan Password	316
Gambar 13 Skema Crack Password dengan Malware.....	335
Gambar 14 MITM Replay	337
Gambar 15 Opening Serangan Web & Aplikasi Server	351
Gambar 16 Cara Kerja Web Server.....	355
Gambar 17 Diagram Alur Server Web.....	362
Gambar 18 Skema Pembajakan Server DNS	368
Gambar 19 Skema Serangan SSH Server.....	375
Gambar 20 Skema Serangan SSRF.....	382
Gambar 21 Screen Shot MetaSploit on ECC Lab EC Council	386
Gambar 22 Arsitektur Apk Web	399
Gambar 23 Cara Kerja Aplikasi Web	401
Gambar 24 Layanan Web	409
Gambar 25 Screen Shoot Parrot Terminal di ECC Labs EC Council	464
Gambar 26 Network Level Attack Opening	475
Gambar 27 Skema Sniffing	481
Gambar 28 Cara Kerja Sniffing.....	484
Gambar 29 Sniffing Pasif	489
Gambar 30 Pembajakan alamat MAC	500
Gambar 31 Serangan DHCP Starvation	505
Gambar 32 Duplikasi Alamat MAC	511
Gambar 33 Ilustrasi Request DNS Normal.....	514

Gambar 34 Ilustrasi Request DNS yang telah kena Poison.....	515
Gambar 35 Skema Serangan DoS.....	526
Gambar 36 Skema Serangan DDoS	528
Gambar 37 Pembajakan UDP	534
Gambar 38 Skema Peer to peer	540
Gambar 39 Low Orbit Ion Cannon (LOIC).....	548
Gambar 40 Skema Pembajakan Sesi.....	559
Gambar 41 Skema Pembajakan atau Hijacking	570
Gambar 42 Skema atau alur Spoofing	573

DAFTAR TABEL

Tabel 1 Perbedaan Virus & Worms.....	155
Tabel 2 Perbandingan Audit Keamanan, Evaluasi Kerentanan, Pentesting	598

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).