

## DAFTAR ISTILAH

<b>Istilah</b>	<b>Keterangan</b>	<b>Pemakaian Pertama Kali pada Halaman</b>
<i>SQL Injection</i>	Salah satu jenis serangan injeksi kode yang menyerang lapisan sistem basis data.	1
<i>Website</i>	Kumpulan halaman web yang saling terhubung dan seluruh file saling terkait.	1
<i>Web Application</i>	<i>Software</i> berbasis web dan dapat diakses melalui browser dengan menggunakan internet.	1
<i>Exploitation</i>	Tahapan Metode PTES dimana penguji mencoba melewati batasan keamanan sistem dengan memaksa mengakses sistem maupun sumber daya yang ada.	2
<i>Penetration Testing Execution Standard (PTES)</i>	Metode atau <i>framework Penetration Testing</i> dengan tujuan menjawab kebutuhan akan standar yang lengkap dan terkini.	2
<i>Security Mitigation</i>	Strategi untuk membatasi dampak ancaman terhadap data yang disimpan.	2
<i>Security Testing</i>	Proses yang menguji seberapa tinggi tingkat keamanan suatu aplikasi web sehingga diketahui nilai dan rekomendasi keamanan yang diberikan.	2
<i>Penetration Testing</i>	Proses simulasi penyerangan ke sistem informasi perusahaan untuk mengeksploitasi celah kerentanan yang dimiliki.	3
<i>Reporting</i>	Tahapan Metode PTES dengan menuliskan	3

	dokumentasi seluruh proses lengkap pengujian yang telah dilakukan dalam bentuk laporan.	
<i>Hyperlink</i>	Teks berupa <i>link</i> yang menghubungkan satu sama lain, seperti file ataupun halaman <i>website</i> .	8
<i>Hostile Data</i>	Data yang digunakan penyerang bertujuan merusak, misalnya <i>payload</i> jahat	9
<i>Domain</i>	Nama unik yang diberikan untuk alamat IP fisik di internet.	10
<i>Host</i>	Sistem pada server yang saling berhubungan satu sama lain.	10
<i>IP Address</i>	Label numerik yang menjadi identitas perangkat yang terhubung ke internet atau infrastruktur jaringan lainnya.	10
<i>Proxy</i>	<i>Intermediary</i> antara browser klien dengan <i>resources</i> .	11
<i>Black Box</i>	Salah satu teknik pengujian dimana penguji tidak memiliki pengetahuan apapun tentang arsitektur atau sistem jaringan pengujian	12
<i>Grey Box</i>	Salah satu teknik pengujian dimana penguji memiliki sebagian pengetahuan tentang jaringan atau beberapa informasi dasar tentang pengujian jaringan dan konfigurasi sistem.	13
<i>White Box</i>	Salah satu teknik pengujian dimana penguji memiliki seluruh pengetahuan tentang konfigurasi jaringan dan konfigurasi sistem jaringan/sistem pengujian.	13
<i>Pre-engagement Interactions</i>	Tahapan Metode PTES dimana penguji mempersiapkan dan mengumpulkan alat pengujian, perangkat, teknik yang digunakan, serta dokumen pengujian.	14
<i>Intelligence Gathering</i>	Tahapan Metode PTES dimana dilakukan	14

	pengumpulan informasi yang digunakan dalam <i>Penetration Testing</i> .	
<i>Threat Modelling</i>	Tahapan Metode PTES dimana dilakukan pemodelan ancaman sebagai bentuk optimalisasi sistem agar dapat mengidentifikasi kerentanan.	14
<i>Vulnerability Analysis</i>	Tahapan Metode PTES dimana dilakukan proses pengujian celah keamanan untuk menemukan kerentanan suatu sistem dan aplikasi.	14
<i>Post Exploitation</i>	Tahapan Metode PTES dimana penguji menentukan nilai dari target yang akan diuji serta mempertahankan kontrol atas sistemnya.	15
<i>Design Science</i>	Salah satu paradigma dari Model Konseptual Hevner yang dimana <i>Design Science</i> melakukan perancangan dengan tujuan mengatasi keterbatasan kemampuan manusia dan organisasi dengan cara memanfaatkan teknologi informasi.	16
<i>Behaviour-Science</i>	Salah satu paradigma dari Model Konseptual Hevner yang dimana <i>Behaviour-Science</i> melakukan pengembangan dan memodifikasi teori yang menjelaskan serta memprediksi perilaku manusia atau organisasi.	16
<i>Environment</i>	Bagian dari Metode Konseptual yang berupa lingkup kondisi dari permasalahan dari sebuah penelitian.	17
<i>Evaluation</i>	Pengujian terhadap solusi yang memungkinkan untuk dapat dilakukan implementasi.	17
<i>Foundations</i>	Bagian dari <i>Knowledge Base</i> dalam Metode Konseptual berupa dasar ilmu teori penelitian.	17

<i>Knowledge Base</i>	Bagian dari Metode Konseptual yang berupa teori yang dijadikan sebagai acuan dalam penelitian.	17
<i>Object Relational Mapping (ORM)</i>	Teknik yang menghubungkan tabel basis data dengan kode pemrograman objek agar mudah mengakses <i>database</i> tanpa melakukan <i>query</i> secara manual.	157
<i>Web Application Firewall (WAF)</i>	<i>Firewall</i> yang menyaring, memantau, dan memblokir lalu lintas HTTP ke dan dari layanan web.	157
<i>Profiling</i>	Langkah dalam menentukan karakteristik untuk mengenali suatu sistem	162