

DAFTAR ISTILAH

Istilah	Deskripsi	Halaman pertama kali digunakan
<i>Website</i>	Kumpulan halaman yang digunakan untuk menampilkan informasi teks, gambar, animasi suara, atau dari gabungan semuanya baik yang bersifat statis atau dinamis.	1
<i>Vulnerability</i>	Kerentanan atau kelemahan yang terjadi akibat cacat sistem ataupun infrastruktur yang digunakan.	2
VAPT	<i>Vulnerability Assessment and Penetration Testing</i> adalah sebuah metode yang digunakan untuk mengevaluasi suatu sistem atau jaringan dan menguji kemampuannya untuk mempertahankan diri terhadap serangan yang sengaja dilakukan.	2
<i>Security Testing</i>	Pengujian perangkat lunak atau sistem untuk mengidentifikasi kerentanan atau celah keamanan.	2
Eksploitasi	Tindakan dengan atau tanpa persetujuan korban yang sifatnya untuk keuntungan pribadi.	2
<i>Server</i>	Sistem komputer yang menjalankan jenis layanan tertentu dalam sebuah jaringan komputer dan menyediakan sumber daya untuk penyimpanan data.	2

<i>Vulnerability Assessment</i>	Proses untuk mengidentifikasi, mengevaluasi, dan mengklasifikasikan tingkat risiko pada kerentanan keamanan pada sebuah jaringan komputer, sistem, aplikasi, atau bagian lain yang ada di ekosistem IT.	2
<i>Client</i>	Sebuah aplikasi atau sistem yang mengakses sebuah sistem layanan yang berada di sistem atau komputer lain yang dikenal dengan <i>server</i> melalui jaringan komputer.	2
<i>Existing</i>	Suatu keadaan yang sudah ada	3
<i>Reporting</i>	Suatu bentuk penyampaian berita, keterangan, pemberitahuan ataupun pertanggungjawaban baik secara lisan maupun secara tulisan.	3
<i>Tools</i>	Perangkat lunak atau sistem perangkat keras yang bekerja dalam sebuah proses pengujian.	3
<i>Vulnerability Analysis</i>	Bagian dari siklus <i>vulnerability assessment</i> dengan menyelidiki atau menganalisis kerentanan yang terdeteksi oleh alat yang digunakan saat proses <i>vulnerability assessment</i> .	4
<i>Browser</i>	Perangkat lunak yang digunakan untuk membuka <i>website</i>	5
<i>Firewall</i>	Sebuah sistem atau perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman.	5

<i>Port</i>	Jalur yang digunakan untuk menghubungkan komputer atau <i>server</i> dalam sebuah jaringan.	6
PTES	<i>Penetration Testing Standard</i> .	7
<i>Host</i>	Komputer atau perangkat lain yang berkomunikasi dengan komputer di jaringan lain.	8
<i>IP Address</i>	Identitas angka yang digunakan oleh semua perangkat komputer agar saling berhubungan dalam jaringan internet.	10
<i>Framework</i>	Pendekatan yang ditentukan yang bermaksud sebagai pedoman, standar, dan praktik terbaik dalam melakukan sebuah proses.	11
<i>Domain</i>	Alamat dalam bentuk nama unik pada sebuah <i>website</i> yang berfungsi sebagai jalur komunikasi antara <i>client</i> dan <i>website</i> yang ingin dituju.	22
<i>People</i>	<i>People</i> merujuk pada pihak atau pengguna yang berinteraksi dengan sistem dan data yang diuji dengan tujuan untuk meningkatkan <i>security awareness</i> sehingga dapat menghindari potensi risiko keamanan atau serangan lainnya yang dapat membahayakan keamanan data	23
<i>Technology</i>	<i>Technology</i> mencakup semua perangkat keras dan perangkat lunak yang digunakan dalam pengujian	23
<i>Process</i>	<i>Process</i> merupakan prosedur atau langkah-langkah yang digunakan untuk	23

	mengelola penanganan terhadap sistem yang diuji	
<i>Severity</i>	Tingkatan dalam penilaian risiko terhadap suatu kerentanan.	24
<i>Clickjacking</i>	Teknik serangan yang menyamarkan suatu elemen <i>website</i> guna mengelabui pengguna. Penyerang menggunakan HTML untuk membuat <i>invisible page</i> di atas halaman yang dilihat pengguna.	26
URL	Rangkaian karakter menurut suatu format standar tertentu, yang digunakan untuk menunjukkan alamat suatu sumber, seperti dokumen dan gambar di internet.	26
<i>Cross Site Scripting (XSS)</i>	Eksplorasi keamanan di mana penyerang menempatkan kode berbahaya ke laman <i>website</i> .	28
<i>Confidence</i>	Tingkat kepercayaan atau keyakinan terhadap kerentanan yang ditemukan. Hal ini mencerminkan reliabilitas inheren dari teknik yang digunakan untuk mengidentifikasi masalah.	30
<i>Risk</i>	Tingkat penilaian risiko terhadap kerentanan yang ditemukan.	32
<i>Security</i>	Pengaturan pada suatu fitur <i>automated scanner</i> untuk mengontrol tingkat keamanan ketika melakukan pemindaian pada target	31