DAFTAR ISTILAH

Istilah	Deskripsi	Hal.
Cybercrime	: *Cybercrime* adalah kejahatan yang dilakukan menggunakan teknologi komputer dan internet. Hal ini mencakup berbagai tindakan ilegal seperti peretasan (hacking), pencurian data, penipuan online, serangan siber, dan penyebaran *malware*.	1
Firewall	: *Firewall* adalah sistem keamanan yang berfungsi sebagai penghalang antara jaringan internal dan jaringan eksternal, seperti internet. Fungsinya adalah untuk mengawasi, mengontrol, dan memantau lalu lintas data yang masuk dan keluar dari jaringan, serta mengidentifikasi dan memblokir akses yang mencurigakan atau berbahaya.	1
Aplikasi *Web*	: Aplikasi *web* adalah perangkat lunak yang diakses melalui *browser web* dan berjalan di *server*. Aplikasi ini memungkinkan pengguna untuk berinteraksi, melakukan tugas, dan mendapatkan informasi secara *online* melalui internet.	1
Penyerang	: Penyerang adalah pihak atau individu yang melakukan serangan siber atau mencoba untuk mengakses dan merusak sistem atau aplikasi komputer tanpa izin atau tujuan yang jahat.	1
Post Exploitation	: *Post exploitation* adalah tahap dalam serangan siber setelah penyerang berhasil mengakses dan menguasai sistem atau aplikasi target.	2
Server	: *Server* adalah komputer atau sistem komputer yang menyediakan layanan. Fungsinya adalah untuk mengelola, menyimpan, dan memproses data serta menyediakan layanan dan aplikasi untuk pengguna akhir.	4

Node (Attack Tree)	:	*Node* (a*ttack tree*) adalah representasi visual dari serangan yang mungkin terjadi pada suatu sistem atau aplikasi. Setiap *node* mewakili tindakan atau langkah spesifik dalam serangan yang bertujuan untuk mencapai tujuan penyerang.	5
Core Hardware	:	*Core hardware* adalah perangkat yang menampung dan memberikan sumber daya terhadap virtual *machine* yang ada pada komputer tersebut.	16
Virtual Machine	:	Mesin virtual (*Virtual Machine*) adalah emulasi berbasis perangkat lunak dari sistem komputer yang berjalan di komputer fisik atau *server*. Ini memungkinkan beberapa sistem operasi (OS) atau lingkungan beroperasi secara mandiri pada perangkat keras fisik yang sama.	13
Operating System	:	Sistem operasi (*Operating System*) adalah perangkat lunak yang mengelola dan mengontrol sumber daya komputer, termasuk *hardware, software*, dan proses pengguna.	16
Attack Tools	:	*Attack tools* adalah perangkat lunak atau skrip yang digunakan oleh penyerang dalam serangan siber. Alat-alat ini dirancang untuk mengeksploitasi celah keamanan dalam sistem atau aplikasi komputer, mencuri informasi sensitif, menyebabkan kerusakan, atau mendapatkan akses ilegal ke perangkat atau jaringan.	17
Penetration Testing	:	*Penetration testing* adalah pengujian ketahanan suatu sistem terhadap serangan potensial dan memberikan wawasan tentang area yang perlu diperkuat untuk meningkatkan keamanannya.	17
Model Lapisan OSI	:	Model lapisan OSI (*Open Systems Interconnection*) adalah sebuah konsep standar yang digunakan untuk	19