

DAFTAR ISTILAH

<i>Deauthentication Attack</i>	: Jenis serangan jaringan yang menargetkan komunikasi antara perangkat klien dan titik akses Wi-Fi yang bertujuan untuk memutuskan koneksi perangkat klien [1].
<i>Beacon frame</i>	:Jenis frame manajemen dalam protokol <i>IEEE 802.11</i> yang dikirimkan secara berkala oleh akses point dalam jaringan nirkabel.
<i>Wi-Fi Analyzer</i>	:menganalisis jaringan Wi-Fi yang ada di sekitar jaringan yang memberikan informasi secara detail tentang jaringan <i>Wi-Fi</i> seperti kekuatan sinyal dan channell yang digunakan.
<i>Man-In The-Middle</i>	:Jenis serangan siber dimana penyerang diam diam menyusupkan ke dalam komunikasi antara dua pihak dan dapat memantau, mengubah atau mencuri informasi yang sedang dipertukarkan tanpa sepengetahuan kedua pihak tersebut
<i>Deauth detector</i>	:Perangkat yang digunakan untuk mendeteksi adanya serangan <i>deauthentication</i> pada jaringan <i>Wi-Fi</i> .
<i>Network Penetration Testing</i>	:Proses simulasi serangan yang dilakukan terhadap jaringan komputer untuk mengidentifikasi, mengeksploitasi dan menilai kerentanan keamanan yang ada.
<i>Open System Interconnection</i>	:Model referensi konseptual yang mendefinisikan bagaimana berbagai protokol jaringan berinteraksi dalam komunikasi jaringan komputer.

<i>Management Frame</i>	:Jenis frame dalam protokol <i>IEEE 802.11 (Wi-Fi)</i> yang digunakan untuk mengelola dan memelihara koneksi antar perangkat di jaringan nirkabel.
<i>Access Point</i>	:Perangkat jaringan yang memungkinkan perangkat nirkabel, seperti laptop, smartphone, atau tablet, untuk terhubung ke jaringan kabel melalui sinyal <i>Wi-Fi</i> .
<i>Chip</i>	:Komponen dasar yang terdiri dari resistor, transistor dan lain-lain. Yang dipakai sebagai otak peralatan elektronika.
<i>Select AP</i>	:Memilih titik akses.
<i>Bluetooth</i>	:Teknologi komunikasi nirkabel yang dirancang untuk menghubungkan perangkat elektronik dalam jarak dekat, umumnya hingga sekitar 10 hingga 100 meter.
<i>TimeStamp</i>	:Nilai yang mewakili waktu di titik akses yang merupakan jumlah mikrodetik AP telah aktif
<i>Brute Force</i>	:Teknik serangan dalam keamanan siber di mana penyerang mencoba untuk mendapatkan akses ke suatu sistem, akun, atau data dengan mencoba berbagai kombinasi kemungkinan secara sistematis hingga menemukan kombinasi yang benar.
<i>Packet Monitor</i>	:Untuk mengamati, menangkap dan menganalisis data yang melewati jaringan komputer.
<i>Blue Team</i>	:Team Keamanan yang bertugas melindungi Perusahaan dari ancaman dunia maya.
<i>Cyber Attack</i>	: Tindakan berbahaya yang dilakukan oleh individu atau kelompok untuk merusak, mengganggu, mencuri, atau mengakses data, sistem atau jaringan komputer secara illegal.