DAFTAR ISTILAH

Deauthentication Attack	: Jenis serangan jaringan yang menargetkan komunikasi antara perangkat klien dan titik akses Wi-Fi yang bertujuan untuk memutuskan koneksi perangkat klien [1].
Beacon frame	:Jenis frame manajemen dalam protokol *IEE 802.11* yang dikirimkan secara berkala oleh akses point dalam jaringan nirkabel.
Wi-Fi Analyzer	:menganalisis jaringan Wi-Fi yang ada di sekitar jaringan yang memberikan informasi secara detail tentang jaringan *Wi-Fi* seperti kekuatan sinyal dan channell yang digunakan.
Man-In The-Middle	: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
Deauth detector	:Perangkat yang digunakan untuk mendeteksi adanya serangan *deauthentication* pada jaringan *Wi-Fi*.
Network Penetration Testing	:Proses simulasi serangan yang dilakukan terhadap jaringan komputer untuk mengidentifikasi, mengeksploitasi dan menilai kerentanan keamanan yang ada.
Open System Interconnection	:Model referensi konseptual yang mendefinisikan bagaimana berbagai protokol jaringan berinteraksi dalam komunikasi jaringan komputer.

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