**Mata Kuliah Keamanan Sistem & Jaringan Komputer**

**Dosen : Arief Prasetyo**

**PRAKTIKUM 10**

**KEAMANAN JARINGAN NIRKABEL**

Oleh :



Nama : Rizky Lanang Sadana Mulyono Putra

Kelas : TI-3B

No. Urut : 19

No. HP : +6285794801890

E-mail : [rizkylsmp@gmail.com](mailto:rizkylsmp@gmail.com)

**# Soal Tugas 1**

1. Apakah yang dimaksud jaringan nirkabel?
2. Apa perbedaan jaringan kabel dengan jaringan nirkabel menurut IEEE?
3. Apa yg dimaksud dengan WAP Apa fungsinya?
4. Apakah standar yang menetapkan teknologi WLAN menurut IEEE?
5. Sebutkan dan jelaskan singkat standar teknologi nirkabel lain selain WLAN!
6. Apakah yang dimaksud basic service set dalam konteks wi fi ?
7. Jelaskan salah satu topologi yang ada pada jaringan nirkabel!
8. Apa saja 2 protocol keamanan nirkabel yang umum digunakan saat ini?
9. Kenapa WEP mulai ditinggalkan?
10. Sebutkan dan jelaskan masalah keamanan yang dihadapi dalam penggunaan jaringan nirkabel!

**# Jawaban Tugas 1**

1. Jaringan nirkabel adalah jenis jaringan yang menghubungkan perangkat tanpa menggunakan kabel. Perangkat berkomunikasi melalui sinyal radio atau gelombang lainnya.
2. Menurut IEEE (Institute of Electrical and Electronics Engineers), jaringan kabel menggunakan kabel fisik seperti kabel tembaga atau serat optik untuk menghubungkan perangkat. Sementara itu, jaringan nirkabel menggunakan gelombang radio atau inframerah untuk menghubungkan perangkat tanpa kabel fisik.
3. WAP (Wireless Access Point) adalah perangkat yang memungkinkan perangkat nirkabel seperti laptop atau smartphone untuk terhubung ke jaringan kabel. Fungsinya adalah untuk menghubungkan perangkat ke jaringan internet atau jaringan lokal tanpa kabel.
4. Standar yang menetapkan teknologi WLAN (Wireless Local Area Network) menurut IEEE adalah seri standar IEEE 802.11.
5. Standar teknologi nirkabel selain WLAN :

* Bluetooth (IEEE 802.15.1): Digunakan untuk menghubungkan perangkat jarak dekat seperti headset, keyboard, atau mouse ke komputer atau smartphone.
* WiMAX (IEEE 802.16): Digunakan untuk menyediakan akses internet broadband jarak jauh.
* Zigbee (IEEE 802.15.4): Digunakan dalam aplikasi dengan konsumsi daya rendah seperti sensor rumah pintar dan perangkat IoT (Internet of Things).

1. Basic Service Set (BSS) adalah area yang dicakup oleh satu titik akses nirkabel (WAP) dan perangkat yang terhubung ke titik akses tersebut dalam jaringan Wi-Fi. BSS adalah unit dasar dari jaringan Wi-Fi.
2. Salah satu topologi pada jaringan nirkabel adalah topologi star (bintang). Dalam topologi ini, semua perangkat nirkabel terhubung langsung ke satu titik akses sentral (WAP). WAP ini mengelola komunikasi antara perangkat.
3. Protokol keamanan nirkabel yang umum digunakan saat ini yaitu :

* WPA2 (Wi-Fi Protected Access 2): Protokol keamanan yang paling umum digunakan untuk melindungi jaringan Wi-Fi.
* WPA3 (Wi-Fi Protected Access 3): Versi terbaru dari WPA2 dengan fitur keamanan yang lebih baik.

1. WEP (Wired Equivalent Privacy) mulai ditinggalkan karena memiliki banyak kelemahan keamanan yang mudah ditembus oleh hacker. Ini membuatnya tidak aman untuk melindungi data pada jaringan nirkabel.
2. Masalah keamanan yang dihadapi dalam penggunaan jaringan nirkabel.

* Peretasan (Hacking): Hacker bisa mencoba mengakses jaringan nirkabel yang tidak aman untuk mencuri data.
* Penyadapan (Eavesdropping): Sinyal nirkabel bisa disadap oleh orang yang tidak berwenang untuk mendengarkan komunikasi data.
* Interferensi (Interference): Sinyal nirkabel bisa terganggu oleh perangkat lain seperti microwave atau perangkat elektronik lainnya yang menggunakan frekuensi yang sama.
* Jaringan palsu (Rogue Access Point): Orang jahat bisa memasang titik akses palsu untuk mencuri informasi dari pengguna yang tanpa sadar terhubung ke titik akses tersebut.

**# Soal Tugas 2**

1. Bacalah artikel peretasan keamanan jaringan wireless (WEP WPA password cracking).
2. Buatlah artikel dengan kata kata anda sendiri yang berisi

* Alat dan software apa saja yg dibutuhkan untuk peretasan jaringan nirkabel
* Langkah peretasan jaringan nirkabel

**# Jawaban Tugas 2**

Artikel :

PERETASAN KEAMANAN JARINGAN NIRKABEL: ALAT DAN LANGKAH-LANGKAH

Alat dan Software yang Dibutuhkan untuk Peretasan Jaringan Nirkabel

1. Komputer/Laptop: Perangkat keras utama yang akan digunakan untuk menjalankan software peretasan.
2. Kali Linux: Sistem operasi berbasis Linux yang dilengkapi dengan berbagai alat untuk pengujian penetrasi dan keamanan.
3. Adaptor Wi-Fi yang Mendukung Mode Monitor: Adaptor Wi-Fi eksternal yang mampu beroperasi dalam mode monitor untuk menangkap paket data yang lewat di udara.
4. Aircrack-ng: Suite perangkat lunak yang digunakan untuk menganalisis dan memecahkan kunci jaringan Wi-Fi.
5. Airodump-ng: Bagian dari Aircrack-ng suite yang digunakan untuk menangkap paket data dari jaringan Wi-Fi.
6. Aireplay-ng: Alat untuk menghasilkan lalu lintas yang diperlukan dalam beberapa metode peretasan.
7. Wordlist: Daftar kata yang berisi kemungkinan password yang akan digunakan untuk serangan brute-force.