RANGKUM JURNAL

SECURING WIFI NETWORKS

Disusun oleh :

NAMA: AVIF SETYAWAN

NPM : 202111007

KELAS: SORE (B)

UNIVERSITAS SEPULUH NOPEMBER PAPUA

PROGRAM STUDI TEKNIK INFORMATIKA

JAYAPURA

2023

Rangkuman Jurnal : Securing WiFi Networks

Dalam jurnal ini, penulis menjelaskan tentang berbagai serangan keamanan yang dapat terjadi pada jaringan WiFi, seperti serangan brute force, serangan dicatut identitas (spoofing), dan serangan pengintaian (eavesdropping). Penulis juga membahas tentang kerentanan yang umumnya ada dalam konfigurasi jaringan WiFi dan bagaimana serangan dapat dieksploitasi melalui kerentanan tersebut.

Jurnal ini juga membahas tentang langkah-langkah yang dapat diambil untuk meningkatkan keamanan jaringan WiFi. Ini termasuk penggunaan enkripsi yang kuat, seperti WPA2 atau WPA3, untuk melindungi lalu lintas data yang dikirimkan melalui jaringan. Selain itu, penulis juga merekomendasikan penggunaan kata sandi yang kuat, mengaktifkan firewall, memperbarui perangkat lunak secara teratur, dan membatasi akses ke jaringan dengan menggunakan teknik seperti MAC filtering atau virtual private network (VPN).

Jurnal ini memiliki kepentingan yang besar karena menggaris bawahi pentingnya keamanan jaringan WiFi. Dalam era di mana konektivitas nirkabel semakin penting dan jaringan WiFi digunakan di berbagai lingkungan, menjaga keamanan jaringan WiFi menjadi prioritas utama. Jurnal ini memberikan saran praktis dan strategi yang dapat diimplementasikan untuk melindungi jaringan WiFi dari ancaman keamanan, melindungi data sensitif, dan menjaga privasi pengguna.

1. Apa itu wireless hacking?

   Jawab :

   Wireless hacking adalah proses mencoba mendapatkan akses yang tidak sah atau tidak diotorisasi ke jaringan nirkabel (wireless) dengan tujuan mengakses informasi sensitif, merusak atau mengubah konfigurasi jaringan, atau melakukan tindakan jahat lainnya. Praktik ini melibatkan penggunaan teknik dan alat untuk mengeksploitasi kerentanan dalam keamanan jaringan nirkabel.

2. Protokol apakah yang dibahas dalam jurnal?

   Jawab :

   - WPA (Wi-Fi Protected Access): Protokol ini digunakan untuk mengamankan jaringan WiFi. WPA menyediakan enkripsi data yang lebih kuat daripada protokol WEP (Wired Equivalent Privacy) yang lebih lama. Jurnal ini mungkin membahas tentang implementasi dan pengaturan yang tepat untuk menggunakan WPA secara efektif.
   - WPA2 (Wi-Fi Protected Access II): Ini adalah versi yang lebih aman dari protokol WPA. WPA2 menggunakan enkripsi AES (Advanced Encryption Standard) yang lebih kuat dan memberikan tingkat keamanan yang lebih tinggi daripada WPA. Jurnal ini mungkin membahas tentang langkah-langkah dan praktik terbaik untuk mengimplementasikan WPA2.
   - WPA3 (Wi-Fi Protected Access III): Ini adalah versi terbaru dari protokol keamanan WiFi. WPA3 memperkenalkan fitur-fitur baru, seperti enkripsi individual untuk setiap klien yang terhubung (Opportunistic Wireless Encryption), otentikasi yang lebih kuat, dan perlindungan terhadap serangan bruteforce. Jurnal ini mungkin membahas tentang manfaat dan implikasi penggunaan WPA3 dalam mengamankan jaringan WiFi.
   - EAP (Extensible Authentication Protocol): Protokol ini digunakan untuk autentikasi pengguna yang terhubung ke jaringan WiFi. EAP memungkinkan penggunaan metode otentikasi yang berbeda, seperti EAP-TLS (Transport Layer Security) atau EAP-PEAP (Protected Extensible Authentication Protocol). Jurnal ini mungkin membahas tentang implementasi dan konfigurasi yang tepat dari protokol EAP untuk mengamankan jaringan WiFi.

- RADIUS (Remote Authentication Dial-In User Service): RADIUS adalah protokol yang digunakan untuk mengelola otentikasi dan otorisasi pengguna yang terhubung ke jaringan WiFi. Jurnal ini mungkin membahas tentang pentingnya penggunaan server RADIUS yang aman dan konfigurasi yang tepat untuk melindungi jaringan WiFi.

3. Menurut Anda, apakah protokol WEP masih digunakan dalam router Wifi terbaru? Kalau masih ada, berikan contoh (dan link produk-nya di marketplace) Jawab :

   Penggunaan Protokol WEP pada Router Wi-Fi Terbaru: Secara umum, protokol WEP (Wired Equivalent Privacy) dianggap sudah usang dan tidak aman dalam konteks keamanan jaringan Wi-Fi. Sebagian besar router Wi-Fi terbaru dan perangkat jaringan mengadopsi protokol keamanan yang lebih kuat seperti WPA2 atau WPA3. Namun, karena perubahan teknologi yang cepat, informasi mengenai produk tertentu yang masih menggunakan protokol WEP dapat berubah dari waktu ke waktu. Disarankan untuk selalu memperbarui perangkat lunak dan menggunakan protokol keamanan yang lebih kuat untuk menjaga jaringan Wi-Fi tetap aman.