MODUL PERKULIAHAN:
KEAMANAN SIBER

Penyusun 1	Penyusun 2	Penyusun 3
Denpasar, <*Arial, 9pt>	Denpasar, <*Arial, 9pt>	Denpasar,
(Nama Dosen dan gelar) <*Arial, 9pt>	(Nama Dosen dan gelar) <*Arial, 9pt>	Nama Dosen dan gelar) <*Arial, 9pt>

INFORMASI MATA KULIAH

Jumlah SKS	**4**
Jenis Matakuliah	Teori
Kegiatan Pembelajaran	Daring
Persyaratan Sarana Peserta/Spesifikasi/ Tools/Media ajar yang akan digunakan	

CAPAIAN DAN DESKRIPSI MK

Capaian Pembelajaran Mata Kuliah (CPMK)	Deskripsi Singkat MK
• CPMK-06-17: Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi. • CPMK-07-4: Mampu menjelaskan dan menguasai konsep dasar teori jaringan mahasiswa mampu memahami konsep jaringan komputer, mengetahui perangkat-perangkat jaringan, protokol jaringan, OSI dan TCP/IP model, konsep IP Address dan kelas-kelas dalam IP Address, Routing dengan media virtual seperti menggunakan packet tracer, memahami jaringan nirkabel, mengetahui serangan dalam jaringan dan mengetahui firewall.	Keamanan siber adalah matakuliah yang mempelajari tentang konsep dan teknik untuk pengamanan aplikasi, sistem dan jaringan komputer serta data digital dari kejahatan cyber yang dapat menggangu proses bisnis dan mengakibatkan kerugian.

REFERENSI

Referensi
[1] Sadikin, R. (2012). Kriptografi Untuk Keamanan Jaringan dan Implementasinya dalam bahasa java. Yogyakarta: Andi [2] Weidman, G. (2014). Penetration Testing A Hands-On Introduction to Hacking. [3] Situmeang, M.S (2020). Cyber Law, Bandung: Cakra 2020

Wireless Security

Capaian Pembelajaran Mata Kuliah
• CPMK-06-17: Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi.

Indikator Penilaian
1.1 Pengenalan jaringan wireless 1.2 Kelemahan jaringan wireless 1.3 Wifi Security 1.4 Jenis-jenis serangan jaringan wireless 1.5 Teknik pengamanan jaringan wireless 1.6 Pengujian keamanan wireless

Bab 1: Pengantar Wireless Security

1. Definisi dan Pentingnya Keamanan Jaringan Nirkabel

Pengertian jaringan nirkabel

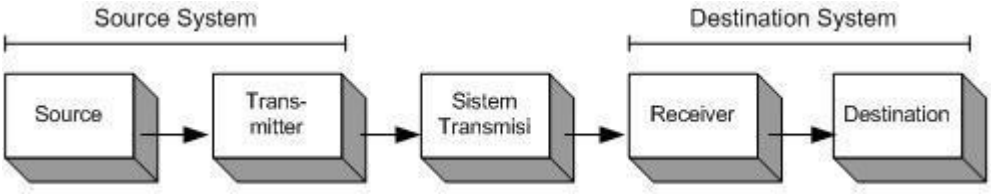
Jaringan nirkabel (*wireless network*) adalah jenis jaringan yang memungkinkan perangkat untuk terhubung dan berkomunikasi tanpa menggunakan kabel fisik, melainkan melalui gelombang radio atau sinyal elektromagnetik. Teknologi ini memungkinkan data untuk ditransmisikan antara perangkat, seperti komputer, ponsel, atau perangkat IoT, melalui sinyal yang dipancarkan melalui udara. Contoh umum dari jaringan nirkabel adalah Wi-Fi, yang digunakan untuk menghubungkan perangkat ke internet di rumah, kantor, atau tempat umum.

Teknologi jaringan nirkabel menggunakan berbagai standar komunikasi, termasuk **IEEE 802.11** untuk Wi-Fi, **Bluetooth** untuk koneksi jarak pendek, dan **LTE/5G** untuk komunikasi seluler. Setiap standar ini memiliki jangkauan dan kecepatan yang berbeda-beda, serta berfungsi untuk memenuhi kebutuhan jaringan dalam berbagai situasi.

Jenis-jenis Jaringan Nirkabel

1. **LAN Nirkabel (WLAN)**
   Biasanya dikenal sebagai jaringan Wi-Fi, WLAN memungkinkan perangkat untuk terhubung ke internet di area tertentu, seperti rumah, kantor, atau tempat umum, dengan menggunakan router sebagai titik akses.
2. **PAN Nirkabel (WPAN)**
   Jaringan ini menghubungkan perangkat dalam jarak dekat, seperti melalui teknologi Bluetooth atau Zigbee, untuk komunikasi jarak pendek seperti antar perangkat pribadi atau untuk aplikasi IoT.
3. **Jaringan Seluler**
   Menggunakan teknologi LTE, 4G, atau 5G untuk memungkinkan komunikasi jarak jauh, jaringan seluler memungkinkan perangkat bergerak untuk tetap terhubung saat berpindah lokasi.
4. **MAN Nirkabel (WMAN)**
   Jaringan ini mencakup area metropolitan yang lebih luas dan biasanya digunakan oleh penyedia layanan internet (ISP) untuk menyediakan akses internet tanpa kabel di area tertentu.

Bagaimana proses komunikasi data terjadi



Komunikasi data adalah proses pertukaran informasi antara dua atau lebih perangkat menggunakan media transmisi, yang bisa berupa kabel (wired) atau gelombang radio (wireless). Proses ini melibatkan beberapa elemen utama: sumber, media transmisi, protokol, dan penerima. Berikut adalah langkah-langkah dasar dalam komunikasi data:

1. **Sumber Mengirimkan Data**
   Perangkat pengirim (sumber) memulai komunikasi dengan mengirimkan data yang dikodekan dalam bentuk sinyal. Pada jaringan nirkabel, data dikonversi menjadi sinyal radio atau gelombang elektromagnetik.
2. **Enkapsulasi dan Pengkodean Data**
   Data dikemas atau dienkapsulasi dalam bentuk paket oleh protokol jaringan (seperti TCP/IP) yang berfungsi untuk menentukan bagaimana data tersebut dipisahkan menjadi bagian-bagian kecil yang dapat ditransmisikan dan diterima dalam urutan yang benar.
3. **Penggunaan Media Transmisi**
   Data dikirimkan melalui media transmisi yang dipilih. Pada jaringan nirkabel, media transmisi adalah udara, di mana sinyal gelombang radio membawa data dari sumber ke penerima melalui frekuensi yang disesuaikan.
4. **Protokol untuk Pengaturan Komunikasi**
   Protokol, seperti TCP/IP untuk internet dan IEEE 802.11 untuk Wi-Fi, mengatur komunikasi data antara perangkat. Protokol ini memastikan bahwa data dikirimkan, diterima, dan diuraikan dengan benar.
5. **Penerimaan dan Dekode Data oleh Penerima**
   Perangkat penerima menerima sinyal dan mendekodekannya kembali menjadi data yang dapat dipahami. Proses dekapsulasi terjadi di sini, di mana data yang diterima dibuka dari kemasan paketnya agar dapat digunakan oleh aplikasi.
6. **Konfirmasi dan Tanggapan**
   Jika data diterima dengan benar, penerima dapat mengirimkan sinyal konfirmasi kembali ke pengirim. Ini memastikan bahwa pengirim tahu bahwa pesan telah sampai dengan benar.

Definisi Keamanan Jaringan Nirkabel

Keamanan jaringan nirkabel (*wireless security*) adalah upaya untuk melindungi jaringan komunikasi nirkabel dari ancaman yang dapat membahayakan data atau akses pengguna. Dalam jaringan nirkabel, data dikirim melalui gelombang radio, sehingga lebih rentan terhadap serangan daripada jaringan berkabel, yang membutuhkan koneksi fisik. Oleh karena itu, keamanan jaringan nirkabel melibatkan berbagai metode dan protokol, seperti enkripsi, autentikasi, dan kontrol akses, yang dirancang untuk melindungi data yang ditransmisikan dan mencegah akses yang tidak sah.

Pentingnya Keamanan Jaringan Nirkabel

1. **Melindungi Data Pribadi dan Sensitif**
   Dalam jaringan nirkabel, data pribadi, informasi keuangan, dan data bisnis sering kali ditransmisikan antara perangkat. Tanpa keamanan yang memadai, informasi ini rentan terhadap pencurian data oleh pihak yang tidak berwenang, seperti melalui serangan *man-in-the-middle* atau penyadapan (*eavesdropping*). Keamanan jaringan nirkabel yang kuat membantu memastikan bahwa data yang dikirim tetap aman dan hanya bisa diakses oleh pihak yang sah.
2. **Mencegah Akses Tidak Sah**
   Akses tidak sah dapat menyebabkan berbagai risiko, termasuk pencurian bandwidth, pelanggaran data, atau bahkan penyerangan jaringan. Dengan menerapkan autentikasi pengguna yang kuat dan menggunakan protokol keamanan seperti WPA3,

jaringan nirkabel bisa membatasi akses hanya untuk perangkat yang diizinkan, sehingga mengurangi risiko akses oleh pengguna atau perangkat yang tidak dikenal.

3. **Menjaga Kinerja dan Kualitas Jaringan**
   Serangan pada jaringan nirkabel, seperti *denial-of-service (DoS)*, bisa memperlambat atau bahkan menghentikan fungsi jaringan. Dengan sistem keamanan yang efektif, seperti firewall dan pemantauan jaringan, organisasi dapat mendeteksi serangan lebih awal dan mencegah penurunan kualitas layanan.
4. **Mencegah Dampak Ekonomi dan Reputasi**
   Kebocoran data yang disebabkan oleh kurangnya keamanan jaringan dapat berdampak serius pada reputasi bisnis dan kepercayaan pelanggan. Selain itu, insiden keamanan sering kali berujung pada kerugian finansial, baik dari segi biaya perbaikan, pembayaran tebusan (pada kasus ransomware), atau potensi denda hukum terkait pelanggaran data.
5. **Mengikuti Regulasi dan Standar Keamanan**
   Beberapa industri diwajibkan untuk mematuhi standar keamanan tertentu, seperti GDPR di Eropa dan HIPAA di Amerika Serikat. Standar ini menuntut pengamanan data yang ditransmisikan melalui jaringan nirkabel. Dengan menerapkan keamanan jaringan yang sesuai, organisasi dapat memastikan kepatuhan pada standar dan menghindari penalti

Protokol dan Standar Jaringan Nirkabel

Dalam jaringan nirkabel, protokol dan standar berfungsi sebagai aturan yang memungkinkan perangkat untuk berkomunikasi secara efektif. Protokol ini mengatur cara perangkat berkomunikasi, sementara standar menjamin kompatibilitas perangkat dari berbagai produsen. Berikut ini adalah beberapa protokol dan standar utama yang digunakan dalam jaringan nirkabel:

1. IEEE 802.11 (Wi-Fi)

IEEE 802.11 adalah standar utama untuk jaringan area lokal nirkabel (WLAN) yang biasa dikenal sebagai Wi-Fi. Standar ini mengatur cara perangkat berkomunikasi melalui frekuensi radio dan telah berkembang dalam berbagai versi untuk meningkatkan kecepatan, jangkauan, dan keamanan:

- **802.11a**: Beroperasi pada frekuensi 5 GHz dengan kecepatan hingga 54 Mbps, tetapi dengan jangkauan lebih pendek.
- **802.11b**: Beroperasi pada 2,4 GHz, dengan kecepatan maksimum 11 Mbps dan jangkauan lebih luas.
- **802.11g**: Menggabungkan kecepatan 54 Mbps pada 2,4 GHz, mendukung lebih banyak perangkat dengan jangkauan luas.
- **802.11n (Wi-Fi 4)**: Beroperasi pada 2,4 GHz dan 5 GHz, menggunakan teknologi MIMO (Multiple Input Multiple Output) untuk meningkatkan kecepatan hingga 600 Mbps.
- **802.11ac (Wi-Fi 5)**: Beroperasi pada 5 GHz dengan kecepatan yang lebih tinggi hingga 1 Gbps, mendukung teknologi *beamforming* untuk sinyal lebih stabil.
- **802.11ax (Wi-Fi 6)**: Meningkatkan kapasitas dan efisiensi untuk jaringan padat dengan kecepatan hingga 10 Gbps.

2. WPA (Wi-Fi Protected Access)

WPA adalah protokol keamanan untuk melindungi jaringan Wi-Fi. WPA telah mengalami beberapa pengembangan untuk meningkatkan keamanan:

- **WPA**: Menggunakan enkripsi TKIP (Temporal Key Integrity Protocol) untuk melindungi data.
- **WPA2**: Menggunakan enkripsi AES (Advanced Encryption Standard), yang lebih aman dan lebih sulit untuk ditembus.
- **WPA3**: Menyediakan keamanan lebih tinggi dengan enkripsi 192-bit dan *forward secrecy*, yang melindungi data meski kunci di masa depan dipecahkan.

3. Bluetooth (IEEE 802.15.1)
Bluetooth adalah standar untuk komunikasi jarak pendek dan efisien dalam energi antara perangkat seperti ponsel, komputer, dan perangkat IoT. Bluetooth menggunakan protokol FHSS (Frequency Hopping Spread Spectrum) pada frekuensi 2,4 GHz dan memungkinkan transfer data dan komunikasi antar perangkat yang berada dalam jangkauan sekitar 10 meter (Bluetooth Low Energy atau BLE memiliki jangkauan lebih besar dan lebih hemat daya).

4. Zigbee (IEEE 802.15.4)
Zigbee adalah standar yang dirancang untuk komunikasi nirkabel pada perangkat dengan konsumsi daya rendah, seperti perangkat rumah pintar dan IoT. Zigbee menggunakan frekuensi 2,4 GHz dengan jangkauan hingga 100 meter dalam jaringan *mesh*, yang memperpanjang jangkauan komunikasi melalui perangkat lain.

5. LTE dan 5G
LTE (Long Term Evolution) dan **5G** adalah standar untuk komunikasi seluler yang menawarkan jangkauan luas dan kecepatan tinggi. LTE dan 5G memungkinkan perangkat bergerak untuk tetap terhubung ke internet di area yang luas dan mendukung aplikasi data-intensif seperti streaming video dan aplikasi realitas virtual.

6. Near Field Communication (NFC)
NFC adalah standar komunikasi jarak pendek yang bekerja dalam jarak beberapa sentimeter. NFC sering digunakan dalam pembayaran nirkabel, seperti pada kartu kredit atau ponsel untuk transaksi aman. Protokol ini menyediakan komunikasi dua arah namun memiliki jangkauan yang sangat terbatas, sehingga cocok untuk aplikasi yang membutuhkan jarak dekat dan keamanan tinggi.

7. Infrared (IrDA)
IrDA (Infrared Data Association) adalah standar komunikasi nirkabel yang menggunakan sinar inframerah untuk pertukaran data. Meskipun jarak terbatas dan memerlukan garis pandang langsung, teknologi ini masih digunakan dalam perangkat tertentu, terutama untuk komunikasi sederhana dan transfer data pada perangkat jarak dekat.

Bab 2: Ancaman pada Jaringan Nirkabel

1. Evil Twin Attack

Attacker membuat *access point* palsu yang menyerupai jaringan asli, dengan nama SSID yang sama. Pengguna yang tidak waspada dapat terhubung ke jaringan palsu ini, memungkinkan penyerang untuk memonitor atau mencuri data yang dikirimkan. Data pribadi dan informasi sensitif, seperti kredensial login, bisa dicuri dengan mudah jika pengguna terhubung ke jaringan palsu.

2. Man-in-the-Middle (MitM) Attack

Attacker berada di antara dua perangkat yang sedang berkomunikasi, sehingga dapat memantau dan memodifikasi data yang dikirimkan antara kedua perangkat tersebut. MitM dapat menyebabkan pencurian data, seperti informasi pribadi dan kata sandi, serta memungkinkan penyerang untuk menyisipkan kode berbahaya dalam komunikasi.

3. Wardriving dan Eavesdropping

Wardriving adalah praktik mengumpulkan informasi tentang jaringan nirkabel di suatu area dengan bergerak menggunakan perangkat yang scanning sinyal Wi-Fi. *Eavesdropping* adalah upaya untuk menangkap data yang dikirim melalui jaringan nirkabel tanpa izin. Informasi yang terkumpul dapat digunakan untuk menemukan jaringan yang rentan dan memungkinkan pencurian data atau akses tidak sah ke jaringan.

4. Denial of Service (DoS) Attack

Serangan DoS pada jaringan nirkabel bertujuan untuk mengganggu koneksi atau memutuskan akses pengguna dengan cara membanjiri jaringan dengan lalu lintas palsu atau mengganggu frekuensi yang digunakan. Jaringan menjadi tidak bisa diakses oleh pengguna yang sah, mengakibatkan gangguan pada layanan atau hilangnya koneksi.

5. Password Cracking

Attacker mencoba menebak atau memecahkan kata sandi jaringan nirkabel menggunakan berbagai teknik, seperti *brute-force* atau *dictionary attacks*. Jika kata sandi jaringan lemah, penyerang dapat dengan mudah mengakses jaringan. Jika penyerang berhasil menebak kata sandi, mereka bisa mendapatkan akses penuh ke jaringan, memungkinkan mereka untuk mencuri data atau melakukan serangan lebih lanjut pada perangkat yang terhubung.

6. Phishing dan Spear Phishing Melalui Wi-Fi Publik

Serangan phishing sering terjadi pada jaringan Wi-Fi publik yang tidak aman. Penyerang dapat membuat situs palsu atau mengirim pesan palsu untuk mengelabui pengguna agar memasukkan informasi sensitif mereka. Informasi sensitif, seperti kredensial login dan informasi kartu kredit, bisa dicuri jika pengguna memasukkan data di situs atau layanan palsu.

7. Rogue Access Point

Access point palsu ini dibuat oleh penyerang atau bahkan orang dalam untuk membuka celah bagi akses jaringan tanpa izin. Access point ini bisa menghubungkan perangkat ke jaringan tanpa melalui prosedur keamanan yang tepat. Penyerang bisa mendapatkan akses langsung ke jaringan perusahaan atau organisasi dan melakukan berbagai bentuk serangan, termasuk pencurian data atau injeksi malware.

8. Jamming

Jamming adalah serangan fisik yang menggunakan perangkat yang memancarkan sinyal radio untuk mengganggu frekuensi yang digunakan oleh jaringan nirkabel. Ini sering terjadi di lokasi padat, di mana penyerang mengganggu akses Wi-Fi agar perangkat tidak bisa

terhubung. Mengganggu konektivitas dan mengurangi kinerja jaringan sehingga layanan terhambat atau bahkan terputus.

Bab 3: Teknik Keamanan Jaringan Nirkabel

Berikut adalah teknik utama yang digunakan untuk meningkatkan keamanan jaringan nirkabel:

1. Enkripsi Data

- WPA3
  WPA3 adalah standar keamanan terbaru yang menggunakan enkripsi lebih kuat, menggantikan WPA2. Dengan enkripsi 192-bit untuk enterprise dan *forward secrecy*, WPA3 memberikan perlindungan yang lebih baik terhadap serangan *brute-force* dan mengamankan data meskipun kunci enkripsi masa depan diretas.
- VPN (Virtual Private Network)
  VPN membantu melindungi data yang ditransmisikan dengan mengenkripsi lalu lintas sebelum dikirim melalui jaringan. VPN sangat penting saat menggunakan jaringan Wi-Fi publik, karena mencegah penyadapan dan pengintaian.

2. Menggunakan Firewall

Firewall dapat diimplementasikan untuk memfilter lalu lintas yang masuk dan keluar dari jaringan. Firewall berbasis perangkat keras dan perangkat lunak berfungsi sebagai penghalang untuk memblokir koneksi tidak sah dan mengidentifikasi perilaku mencurigakan, melindungi perangkat dan jaringan dari potensi ancaman.

3. Hidden SSID dan Pembatasan Jangkauan Sinyal

- Hidden SSID
  Dengan menyembunyikan SSID jaringan tidak akan muncul di daftar jaringan Wi-Fi yang tersedia di perangkat pengguna. Ini menambah tingkat keamanan karena membuat jaringan kurang terlihat oleh penyerang.
- Kontrol Jangkauan Sinyal
  Mengurangi kekuatan sinyal untuk membatasi jangkauan dapat membantu mengurangi risiko penyadapan dari luar area yang diinginkan, misalnya hanya mencakup dalam ruang kantor atau rumah saja.

4. Pemantauan Jaringan dan Deteksi Intrusi

- Intrusion Detection System (IDS)
  IDS dapat memonitor lalu lintas jaringan untuk mendeteksi aktivitas mencurigakan atau serangan. Jika mendeteksi perilaku yang tidak biasa, IDS akan memberikan peringatan kepada administrator jaringan untuk segera mengambil tindakan.
- Pemantauan Lalu Lintas Secara Berkala
  Pemantauan lalu lintas memungkinkan administrator jaringan untuk melihat pola atau aktivitas abnormal yang mungkin menunjukkan adanya upaya akses tidak sah atau serangan pada jaringan.

5. Penggunaan MAC Address Filtering

Mengaktifkan filter alamat MAC (Media Access Control) memungkinkan jaringan untuk membatasi perangkat yang dapat terhubung, dengan hanya memperbolehkan perangkat dengan alamat MAC yang telah diotorisasi. Meskipun teknik ini bisa dibobol, namun memberikan lapisan keamanan tambahan.

6. Segmentasi Jaringan

Segmentasi memisahkan jaringan ke dalam beberapa bagian, misalnya untuk jaringan tamu dan jaringan internal. Hal ini membatasi akses tamu atau perangkat IoT hanya pada area yang terbatas dan mencegah mereka dari mengakses jaringan utama. Segmentasi ini juga bisa diterapkan untuk pemisahan jaringan publik dan pribadi.

7. Pembaruan Firmware dan Patch Keamanan

Produsen perangkat jaringan secara rutin merilis pembaruan firmware dan patch keamanan untuk mengatasi kerentanan. Menginstal pembaruan ini secara berkala sangat penting untuk memastikan perangkat dan jaringan terlindungi dari eksploitasi yang baru ditemukan.

Bab 4: Konfigurasi Keamanan Jaringan Nirkabel pada Perangkat

Mengubah Nama SSID (Service Set Identifier)

Gantilah Nama SSID Default: SSID default sering kali mengidentifikasi jenis perangkat dan produsen, yang bisa memberi petunjuk kepada penyerang. Gunakan nama yang tidak terlalu mengungkap informasi tentang pemilik atau jenis perangkat.
Sembunyikan SSID: Menyembunyikan SSID membuat jaringan tidak terdeteksi secara langsung, meskipun perangkat masih dapat mengaksesnya dengan memasukkan nama SSID secara manual.

Menggunakan Enkripsi WPA3 atau WPA2

Aktifkan WPA3 atau WPA2-Personal
Pilihlah WPA3 sebagai opsi keamanan terbaik (jika perangkat mendukungnya), atau WPA2 jika WPA3 belum tersedia. Hindari WEP (Wired Equivalent Privacy) karena sangat rentan terhadap serangan. Gunakan Kata Sandi yang Kuat: Pilih kata sandi yang panjang, kompleks, dan unik untuk melindungi jaringan dari akses yang tidak sah.

Mengaktifkan MAC Address Filtering

Filter Alamat MAC: Filter alamat MAC hanya mengizinkan perangkat tertentu untuk terhubung ke jaringan. Konfigurasi ini bisa diatur melalui pengaturan router dengan memasukkan alamat MAC dari perangkat yang diizinkan untuk mengakses jaringan.

Mengatur Firewall pada Router

Aktifkan Firewall Router: Firewall pada router dapat membantu memblokir lalu lintas mencurigakan dan melindungi jaringan dari ancaman eksternal. Konfigurasi firewall bisa dilakukan melalui panel administrasi router.
Gunakan Firewall Tambahan pada Perangkat: Mengaktifkan firewall di setiap perangkat yang terhubung akan menambah lapisan perlindungan, terutama jika perangkat sering digunakan untuk aktivitas online di jaringan yang berbeda.

Mengaktifkan VPN (Virtual Private Network)

Gunakan VPN pada Router atau Perangkat: VPN mengenkripsi seluruh lalu lintas jaringan dan melindungi data yang dikirimkan. Beberapa router memungkinkan pemasangan VPN, atau Anda bisa menginstal VPN di perangkat untuk perlindungan saat menggunakan Wi-Fi publik.

Update Firmware Router dan Patch Keamanan

Rutin Meng-update Firmware: Produsen router secara berkala merilis firmware terbaru untuk mengatasi kerentanan keamanan. Pastikan untuk memeriksa dan menginstal pembaruan firmware secara rutin.
Otomatisasi Pembaruan pada Perangkat yang Mendukung: Beberapa router memiliki opsi untuk mengaktifkan pembaruan otomatis, yang bisa membantu memastikan perangkat selalu dilindungi dengan patch terbaru.

Nonaktifkan Fitur yang Tidak Digunakan

Nonaktifkan WPS (Wi-Fi Protected Setup): WPS mempermudah penyerang untuk mencoba menebak kode PIN dan mengakses jaringan. Nonaktifkan WPS di router untuk mengurangi risiko serangan.

Matikan Remote Management: Nonaktifkan akses jarak jauh pada router jika tidak digunakan untuk mencegah akses oleh pihak luar.

Segmentasi Jaringan (Guest Network)

Buat Jaringan Tamu: Jika router mendukungnya, buat jaringan terpisah untuk tamu. Ini akan memisahkan akses antara perangkat internal dan tamu, mencegah mereka mengakses perangkat atau data pribadi di jaringan utama.

Atur Batas Bandwidth dan Akses: Beberapa router memungkinkan untuk mengatur batas kecepatan dan akses pada jaringan tamu. Ini akan menjaga kinerja jaringan utama dan membatasi penggunaan jaringan oleh perangkat tamu.

Menyesuaikan Jangkauan Sinyal

Atur Kekuatan Transmisi Sinyal: Pada beberapa router, Anda dapat mengatur kekuatan sinyal untuk mengurangi jangkauan Wi-Fi. Ini dapat membantu mengurangi kemungkinan akses dari perangkat yang berada di luar area yang diinginkan.

Tempatkan Router dengan Bijak: Posisikan router di bagian tengah ruangan atau bangunan untuk mengoptimalkan jangkauan ke perangkat dalam gedung dan mengurangi jangkauan keluar yang bisa diakses dari luar.

Aktifkan Pemantauan Jaringan

Pantau Lalu Lintas dan Perangkat Terhubung: Periksa perangkat yang terhubung ke jaringan secara berkala dan amati aktivitas lalu lintas jaringan. Beberapa router memiliki fitur pemantauan yang memudahkan untuk memantau aktivitas mencurigakan.

Gunakan Aplikasi Keamanan: Aplikasi keamanan tambahan, seperti IDS (Intrusion Detection System), dapat memberi peringatan jika terdeteksi aktivitas yang tidak biasa atau perangkat yang tidak diizinkan mencoba mengakses jaringan.

Bab 5: Alat dan Teknik Pemantauan Jaringan Nirkabel

Wireshark
Penggunaan Wireshark untuk memantau lalu lintas jaringan dan mengidentifikasi aktivitas mencurigakan.
Kismet
Alat pemantauan jaringan nirkabel untuk mendeteksi perangkat dan menganalisis jaringan.
Acrylic Wi-Fi
Alat untuk mendeteksi SSID, kanal yang digunakan, dan tingkat sinyal jaringan nirkabel.
Aircrack-ng
Penggunaan alat ini untuk menganalisis keamanan jaringan nirkabel dan menguji kerentanan jaringan.