Jurnal Komputasi Terdistribusi

Vol.6 No.4, September 2023
ISSN: 27224707

Analisis Keamanan Perangkat Lunak Terhadap Serangan Melalui Jaringan WiFi Publik

Deitje. S. Pongoh[1], **Sulastri Eksan**[2], **Tiku Pairunan**[3]
Politeknik Negeri Manado
E-mail: pongohdeitje@gmail.com[1], sulastrieksan@gmail.com[2],
pairunantoban36@gmail.com[3]

Abstrak

Dalam era digital yang semakin berkembang, konektivitas nirkabel telah menjadi bagian integral dari kehidupan sehari-hari. Jaringan WiFi publik, yang tersedia di berbagai tempat seperti kafe, bandara, pusat perbelanjaan, dan transportasi umum, memungkinkan akses internet yang mudah dan praktis bagi pengguna. Namun, bersamaan dengan manfaatnya, jaringan WiFi publik juga membawa risiko keamanan yang signifikan. Serangan terhadap perangkat dan data melalui jaringan WiFi publik telah menjadi salah satu ancaman utama dalam dunia teknologi informasi. Serangan semacam itu dapat mencakup serangan man-in-the-middle, sniffing data sensitif, akses ilegal ke perangkat, dan bahkan potensi pencurian identitas. Ketergantungan pada perangkat lunak yang rentan terhadap serangan semacam itu dapat mengancam kerahasiaan, integritas, dan ketersediaan data pribadi maupun bisnis. Dalam menghadapi ancaman ini, penting bagi pengguna dan pengembang perangkat lunak untuk memahami kerentanan perangkat lunak yang sering digunakan dalam pengaturan jaringan WiFi publik. Analisis keamanan perangkat lunak dalam konteks ini adalah kunci untuk mengidentifikasi potensi kerentanan, mengembangkan strategi perlindungan yang efektif, dan mengurangi risiko serangan. Dalam penelitian ini, kami akan mengambil pendekatan menyeluruh untuk menganalisis keamanan perangkat lunak yang digunakan dalam lingkungan jaringan WiFi publik. Kami akan mengevaluasi kerentanan yang umumnya terkait dengan perangkat lunak tersebut dan memberikan wawasan tentang praktik terbaik untuk melindungi diri dari serangan yang mungkin terjadi melalui jaringan WiFi publik. Penelitian ini diharapkan akan memberikan pemahaman yang lebih baik tentang ancaman keamanan yang ada dan membantu dalam upaya meningkatkan tingkat keamanan perangkat lunak yang digunakan dalam lingkungan ini.

Kata Kunci *— Jaringan WiFi, Keamanan, Era Digital.*

PENDAHULUAN

Dalam era digital yang semakin terkoneksi, konektivitas nirkabel telah menjadi pemandangan sehari-hari. Jaringan WiFi publik yang tersebar luas, yang dapat ditemukan di kafe, bandara, perpustakaan, dan berbagai tempat umum lainnya, telah memungkinkan akses internet yang mudah dan nyaman bagi jutaan orang di seluruh dunia. Namun, seiring dengan kenyamanan ini, muncul pula ancaman yang signifikan terhadap keamanan perangkat dan data pengguna. Jaringan WiFi publik adalah lingkungan yang rentan terhadap berbagai jenis serangan yang ditujukan untuk mencuri data pribadi, mencurangi informasi, atau merusak

integritas perangkat lunak yang digunakan. Serangan semacam itu, yang mencakup man-in-the-middle attacks, sniffing data sensitif, akses ilegal ke perangkat, dan potensi pencurian identitas, dapat memiliki dampak yang merugikan baik pada individu maupun organisasi. Dalam menghadapi ancaman ini, pemahaman dan analisis yang cermat tentang keamanan perangkat lunak yang sering digunakan dalam pengaturan jaringan WiFi publik menjadi kunci untuk melindungi diri dari serangan tersebut. Perangkat lunak yang rentan terhadap serangan dapat menjadi pintu masuk bagi penyerang yang ingin mengeksploitasi kerentanan tersebut untuk tujuan jahat. Penelitian ini bertujuan untuk melakukan analisis mendalam terhadap keamanan perangkat lunak yang digunakan dalam konteks jaringan WiFi publik. Kami akan mengeksplorasi kerentanan yang mungkin ada dalam perangkat lunak, mengukur tingkat risiko yang terkait, dan mengembangkan strategi perlindungan yang efektif. Selain itu, penelitian ini akan memberikan wawasan tentang praktik terbaik yang dapat diadopsi oleh pengguna dan pengembang perangkat lunak untuk menjaga keamanan dalam penggunaan jaringan WiFi publik. Dalam upaya untuk memahami dan mengatasi ancaman yang terus berkembang di lingkungan jaringan WiFi publik, penelitian ini diharapkan akan memberikan kontribusi yang berharga kepada komunitas keamanan komputer serta memberikan panduan yang bermanfaat bagi individu dan organisasi yang bergantung pada konektivitas nirkabel ini.

METODE

Evaluasi Penggunaan Alat Keamanan (Security Tool Evaluation): Mengevaluasi efektivitas alat keamanan seperti VPN, firewall, atau antivirus dalam melindungi perangkat dari serangan melalui jaringan WiFi publik.

PEMBAHASAN

Dalam penelitian ini, kami telah menjalankan serangkaian analisis keamanan perangkat lunak yang sering digunakan dalam pengaturan jaringan WiFi publik. Hasil analisis kami menunjukkan beberapa temuan signifikan yang relevan untuk pemahaman dan meningkatkan keamanan dalam penggunaan jaringan WiFi publik. Pemahaman terperinci tentang temuan ini adalah sebagai Kerentanan Perangkat Lunak Teridentifikasi Melalui pemindaian rentan dan analisis kode sumber, kami berhasil mengidentifikasi berbagai kerentanan yang ada dalam perangkat lunak yang digunakan dalam jaringan WiFi publik. Ini termasuk kerentanan umum seperti celah keamanan, konfigurasi default yang tidak aman, dan versi perangkat lunak yang sudah usang. Evaluasi Tingkat Risiko Kami melakukan evaluasi tingkat risiko terkait dengan kerentanan yang teridentifikasi. Kami menggunakan kerangka kerja risiko untuk menentukan dampak potensial dari serangan, probabilitas terjadinya serangan, dan tingkat keparahan risiko. Strategi Perlindungan yang direkomendasikan berdasarkan temuan kami. Ini mencakup rekomendasi untuk mengatasi kerentanan, penggunaan alat keamanan seperti VPN dan firewall, serta praktik terbaik yang dapat diadopsi oleh pengguna untuk mengurangi risiko. Pengujian Keamanan Aplikasi Kami juga melakukan pengujian keamanan aplikasi yang terhubung ke jaringan WiFi publik.

Hasil pengujian ini mengungkapkan kerentanan potensial dalam aplikasi tertentu yang dapat dimanfaatkan oleh penyerang.

Kesadaran Keamanan Salah satu tujuan kami adalah meningkatkan kesadaran keamanan di antara pengguna jaringan WiFi publik. Kami menyajikan informasi yang jelas tentang risiko yang ada dan memberikan saran kepada pengguna tentang tindakan yang dapat mereka ambil untuk melindungi diri mereka sendiri.

Rekomendasi Keamanan Kami memberikan rekomendasi konkret untuk pengguna, pengembang perangkat lunak, dan penyedia layanan jaringan WiFi publik. Rekomendasi ini dirancang untuk membantu semua pihak mengambil langkah-langkah proaktif dalam menjaga keamanan. Selain itu, penting untuk diingat bahwa keamanan perangkat lunak adalah upaya yang terus-menerus. Ancaman dan kerentanannya terus berkembang, sehingga pemantauan dan pemutakhiran berkala perlu dilakukan untuk menjaga tingkat keamanan yang optimal. Penelitian ini memberikan kont

ribusi yang berharga dalam memahami dan mengatasi ancaman keamanan yang ada dalam penggunaan jaringan WiFi publik. Semoga hasil analisis ini dapat memberikan manfaat dalam menjaga keamanan perangkat dan data dalam lingkungan yang semakin terkoneksi ini.

Strategi perlindungan dan tindakan keamanan dalam analisis keamanan perangkat lunak terhadap serangan melalui jaringan WiFi publik sangat penting untuk mengurangi risiko dan menjaga keamanan data Anda. Berikut adalah beberapa strategi dan perlindungan yang dapat Anda terapkan:

1. Penggunaan VPN (Virtual Private Network): Menggunakan VPN adalah salah satu langkah terpenting dalam melindungi data Anda di jaringan WiFi publik. VPN mengenkripsi lalu lintas data Anda, sehingga informasi sensitif tidak dapat dengan mudah diakses oleh penyerang.
2. Pembaruan Perangkat Lunak Teratur: Pastikan perangkat lunak di perangkat Anda selalu diperbarui. Pembaruan perangkat lunak sering mengatasi kerentanan keamanan yang baru ditemukan.
3. Aktifkan Firewall:** Aktifkan firewall di perangkat Anda untuk mengawasi dan mengontrol lalu lintas yang masuk dan keluar. Ini dapat membantu mencegah serangan yang tidak diinginkan.
4. Hati-hati dengan Koneksi Terbuka: Hindari mengakses informasi pribadi atau penting saat terhubung ke jaringan WiFi publik yang tidak terenkripsi. Jika memungkinkan, gunakan koneksi yang terenkripsi atau aman.
5. Verifikasi Keamanan Jaringan WiFi: Pastikan Anda terhubung ke jaringan WiFi resmi jika berada di tempat umum seperti bandara atau kafe. Hindari jaringan WiFi palsu yang mungkin dibuat oleh penyerang.
6. Penggunaan Sandi Kuat: Gunakan kata sandi yang kuat dan unik untuk perangkat Anda serta akun online Anda. Jangan gunakan kata sandi yang sama untuk berbagai layanan.
   Pengaturan Keamanan Perangkat: Aktifkan penguncian perangkat, sidik jari, atau pengenalan wajah untuk mengamankan akses fisik ke perangkat Anda.
7. Penggunaan Keamanan Multi-Faktor (MFA): Aktifkan MFA di akun online Anda ketika memungkinkan. Ini menambahkan lapisan keamanan ekstra dengan memerlukan lebih dari sekadar kata sandi untuk mengakses akun Anda.
8. Edukasi Penggunaan Aman: Edukasi diri sendiri dan orang lain tentang praktik keamanan digital yang baik ketika menggunakan jaringan WiFi publik, seperti tidak mengakses rekening bank atau berbagi informasi pribadi yang sensitif.
9. Pemantauan Aktivitas Aneh: Selalu waspada terhadap aktivitas yang tidak biasa atau mencurigakan di perangkat Anda. Jika Anda melihat sesuatu yang aneh, segera ambil tindakan untuk melindungi diri Anda.
10. Pemantauan Lalu Lintas Data: Gunakan alat pemantauan lalu lintas seperti firewall pihak ketiga atau aplikasi keamanan yang dapat membantu Anda melihat apakah ada upaya yang mencurigakan untuk mengakses data Anda.
11. Penyimpanan Data Aman: Hindari menyimpan data sensitif di perangkat seluler yang dapat dengan mudah hilang atau dicuri.

Gunakan penyimpanan awan yang aman atau enkripsi data Anda.Selain strategi di atas, penting juga untuk memahami bahwa keamanan adalah tanggung jawab bersama.Penggunaan

alat keamanan yang tepat dapat sangat membantu dalam mendeteksi, mencegah, atau merespons ancaman keamanan. Berikut adalah beberapa alat keamanan yang dapat digunakan:

1. Antivirus: Program antivirus adalah alat penting untuk melindungi perangkat lunak Anda dari malware dan virus. Pastikan antivirus Anda selalu diperbarui dan aktif.
2. Firewall:** Firewall melindungi perangkat Anda dengan mengontrol lalu lintas masuk dan keluar. Ini dapat membantu mencegah akses yang tidak diinginkan ke perangkat Anda.
3. VPN (Virtual Private Network): VPN adalah alat yang sangat berguna untuk mengenkripsi lalu lintas data Anda dan menyembunyikan alamat IP Anda saat terhubung ke jaringan WiFi publik.
4. Password Manager: Penggunaan manajer kata sandi dapat membantu Anda membuat dan menyimpan kata sandi yang kuat untuk akun Anda. Ini memastikan bahwa Anda memiliki kata sandi yang berbeda untuk setiap layanan yang Anda gunakan.
5. Aplikasi Keamanan Mobile: Ada berbagai aplikasi keamanan yang tersedia untuk perangkat mobile yang dapat membantu melindungi data Anda, termasuk aplikasi antivirus, aplikasi anti-spyware, dan aplikasi pemantauan lalu lintas.
6. Aplikasi Pemantauan Lalu Lintas: Aplikasi pemantauan lalu lintas seperti Wireshark dapat membantu Anda memantau lalu lintas jaringan Anda untuk mendeteksi aktivitas yang mencurigakan.
7. Aplikasi Keamanan Jaringan WiFi: Beberapa aplikasi dapat membantu Anda mengidentifikasi jaringan WiFi yang aman dan memberikan informasi tentang jaringan yang mungkin tidak aman atau palsu.
8. Pemindai Vulnerability (Vulnerability Scanner): Alat ini digunakan untuk melakukan pemindaian perangkat dan perangkat lunak Anda untuk mengidentifikasi kerentanan yang mungkin ada.
9. Pengujian Keamanan Aplikasi (Application Security Testing Tools): Jika Anda mengembangkan perangkat lunak, alat pengujian keamanan aplikasi dapat membantu Anda mengidentifikasi dan memperbaiki kerentanan sebelum perangkat lunak tersebut digunakan dalam jaringan WiFi publik.
10. Password Cracking Detection Tools: Alat ini dapat membantu mendeteksi percobaan retas kata sandi dan upaya masuk yang mencurigakan.
11. Sistem Pemantauan Keamanan (Security Monitoring Systems): Untuk organisasi yang lebih besar, sistem pemantauan keamanan dapat digunakan untuk melacak dan merespons ancaman yang mungkin terjadi di jaringan.
12. Perangkat Enkripsi: Untuk melindungi data yang disimpan pada perangkat Anda, perangkat enkripsi dapat digunakan untuk mengenkripsi data yang sensitif.

Ingatlah bahwa alat keamanan hanya satu aspek dari keamanan yang efektif.

Kombinasikan penggunaan alat keamanan dengan pendidikan keamanan, pemantauan aktif, dan praktik keamanan yang baik untuk menjaga perangkat Anda dan data Anda tetap aman ketika terhubung ke jaringan WiFi publik.

❖ Ciri-Ciri Jika Keamanan Perangkat Lunak Mendapat Serangan Melalui Jaringan Wifi

Beberapa ciri-ciri jika keamanan perangkat lunak mendapat serangan melalui jaringan WiFi yaitu antara lain:

1. Kinerja yang Lambat atau Tidak Normal
   - Perangkat lunak bisa menjadi lambat atau mengalami penurunan kinerja yang drastis karena adanya beban tambahan akibat serangan.
2. Penggunaan Bandwidth yang Tinggi
   - Ada peningkatan tajam dalam penggunaan bandwidth karena aktivitas yang tidak sah atau transfer data yang besar yang dapat menandakan serangan.
3. Akses Tidak Sah
   - Kemampuan untuk mengakses sistem atau data tanpa izin, bahkan dari luar organisasi

atau entitas yang seharusnya tidak memiliki akses.

4. Munculnya Perangkat atau Akun yang Tidak Dikenal
   - Adanya perangkat atau akun yang tidak dikenal atau tidak sah yang muncul.

❖ Dampak Serangan Jaringan Wi-Fi

Serangan sangat berbahaya bagi keamanan perangkat lunak, Berikut beberapa dampak serius jika terjadi penyerangan seperti:

1. Pencurian Data : Penyerang dapat mencuri informasi pribadi, seperti kata sandi, nomor kartu kredit, dan data sensitif lainnya yang dapat digunakan untuk penipuan.
2. Pencemaran Data : Penyerang dapat mengubah atau merusak data yang disimpan pada perangkat yang terhubung ke jaringan Wi-Fi, mengakibatkan kehilangan atau kerusakan data.
3. Penyadapan Komunikasi : Penyerang dapat memantau dan mencuri komunikasi yang terjadi melalui jaringan, termasuk pesan teks, email, atau percakapan online.
4. Akses ilegal ke Perangkat : Penyerang dapat mendapatkan akses ke perangkat yang terhubung ke jaringan, mengendalikan atau mengambil alih perangkat tersebut.
5. Serangan Malware : Penyerang dapat menyebarkan malware atau virus ke perangkat yang terhubung ke jaringan, yang dapat menyebabkan kerusakan sistem atau pencurian informasi.
6. Pengganggu Layanan : Penyerang dapat mengganggu atau menghambat akses ke internet atau layanan tertentu, mengganggu produktivitas dan penggunaan jaringan.
7. Kekacauan Finansial : Serangan yang mengarah pada pencurian informasi keuangan dapat menyebabkan kerugian finansial bagi individu atau organisasi yang terkena dampak.

Penting untuk selalu melindungi jaringan Wi-Fi dengan mengamankan kata sandi, memperbarui perangkat lunak, dan menggunakan tindakan keamanan yang sesuai untuk mencegah serangan ini.

❖ Cara Mengatasi Jika Terjadi Serangan Terhadap Perangkat Lunak

Untuk mengatasi serangan keamanan perangkat lunak melalui jaringan Wi-Fi, kita dapat melakukan langkah-langkah berikut yaitu:

- Pembaruan Perangkat Lunak dan Sistem Operasi

  Pastikan perangkat lunak dan sistem operasi anda selalu diperbarui dengan versi terbaru yang telah memperbaiki keamanannya.
- Gunakan Firewall

  Aktifkan firewall pada perangkat anda untuk menyatukan dan mengendalikan lalu lintas jaringan, mencegah akses yang tidak sah.
- Gunakan Enkripsi Wi-Fi

  Gunakan enkripsi WPA3

KESIMPULAN

Ketergantungan pada perangkat lunak yang rentan terhadap serangan semacam itu dapat mengancam kerahasiaan, integritas, dan ketersediaan data pribadi maupun bisnis.Dalam menghadapi ancaman ini, penting bagi pengguna dan pengembang perangkat lunak untuk memahami kerentanan perangkat lunak yang sering digunakan dalam pengaturan jaringan WiFi publik. Analisis keamanan perangkat lunak dalam konteks ini adalah kunci untuk mengidentifikasi potensi kerentanan, mengembangkan strategi perlindungan yang efektif, dan mengurangi risiko serangan.Dalam penelitian ini, kami akan mengambil pendekatan menyeluruh untuk menganalisis keamanan perangkat lunak yang digunakan dalam lingkungan jaringan WiFi publik. Kami akan mengevaluasi kerentanan yang umumnya terkait dengan perangkat lunak tersebut dan memberikan wawasan tentang praktik terbaik untuk melindungi diri dari serangan yang mungkin terjadi melalui jaringan WiFi publik. Penelitian ini diharapkan

akan memberikan pemahaman yang lebih baik tentang ancaman keamanan yang ada dan membantu dalam upaya meningkatkan tingkat keamanan perangkat lunak yang digunakan dalam lingkungan ini.

Jaringan WiFi publik adalah lingkungan yang rentan terhadap berbagai jenis serangan yang ditujukan untuk mencuri data pribadi, mencurangi informasi, atau merusak integritas perangkat lunak yang digunakan. Dalam menghadapi ancaman ini, pemahaman dan analisis yang cermat tentang keamanan perangkat lunak yang sering digunakan dalam pengaturan jaringan WiFi publik menjadi kunci untuk melindungi diri dari serangan tersebut. Dalam upaya untuk memahami dan mengatasi ancaman yang terus berkembang di lingkungan jaringan WiFi publik, penelitian ini diharapkan akan memberikan kontribusi yang berharga kepada komunitas keamanan komputer serta memberikan panduan yang bermanfaat bagi individu dan organisasi yang bergantung pada konektivitas nirkabel ini. Pemahaman terperinci tentang temuan ini adalah sebagai Kerentanan Perangkat Lunak Teridentifikasi Melalui pemindaian rentan dan analisis kode sumber, kami berhasil mengidentifikasi berbagai kerentanan yang ada dalam perangkat lunak yang digunakan dalam jaringan WiFi publik. Strategi perlindungan dan tindakan keamanan dalam analisis keamanan perangkat lunak terhadap serangan melalui jaringan WiFi publik sangat penting untuk mengurangi risiko dan menjaga keamanan data Anda. Pemantauan Lalu Lintas Data: Gunakan alat pemantauan lalu lintas seperti firewall pihak ketiga atau aplikasi keamanan yang dapat membantu Anda melihat apakah ada upaya yang mencurigakan untuk mengakses data Anda. Aplikasi Keamanan Mobile: Ada berbagai aplikasi keamanan yang tersedia untuk perangkat mobile yang dapat membantu melindungi data Anda, termasuk aplikasi antivirus, aplikasi anti-spyware, dan aplikasi pemantauan lalu lintas. Aplikasi Keamanan Jaringan WiFi: Beberapa aplikasi dapat membantu Anda mengidentifikasi jaringan WiFi yang aman dan memberikan informasi tentang jaringan yang mungkin tidak aman atau palsu. Pengujian Keamanan Aplikasi (Application Security Testing Tools): Jika Anda mengembangkan perangkat lunak, alat pengujian keamanan aplikasi dapat membantu Anda mengidentifikasi dan memperbaiki kerentanan sebelum perangkat lunak tersebut digunakan dalam jaringan WiFi publik. Sistem Pemantauan Keamanan (Security Monitoring Systems): Untuk organisasi yang lebih besar, sistem pemantauan keamanan dapat digunakan untuk melacak dan merespons ancaman yang mungkin terjadi di jaringan. Perangkat Enkripsi: Untuk melindungi data yang disimpan pada perangkat Anda, perangkat enkripsi dapat digunakan untuk mengenkripsi data yang sensitif. Kombinasikan penggunaan alat keamanan dengan pendidikan keamanan, pemantauan aktif, dan praktik keamanan yang baik untuk menjaga perangkat Anda dan data Anda tetap aman ketika terhubung ke jaringan WiFi publik. Penggunaan Bandwidth yang Tinggi * Ada peningkatan tajam dalam penggunaan bandwidth karena aktivitas yang tidak sah atau transfer data yang besar yang dapat menandakan serangan.

Munculnya Perangkat atau Akun yang Tidak Dikenal * Adanya perangkat atau akun yang tidak dikenal atau tidak sah yang muncul. Dampak Serangan Jaringan Wi-Fi Serangan sangat berbahaya bagi keamanan perangkat lunak, Berikut beberapa dampak serius jika terjadi penyerangan seperti: Pencurian Data : Penyerang dapat mencuri informasi pribadi, seperti kata sandi, nomor kartu kredit, dan data sensitif lainnya yang dapat digunakan untuk penipuan.

Untuk mengatasi serangan keamanan perangkat lunak melalui jaringan Wi-Fi, kita dapat melakukan langkah-langkah berikut yaitu: * Pembaruan Perangkat Lunak dan Sistem Operasi -Pastikan perangkat lunak dan sistem operasi anda selalu diperbarui dengan versi terbaru yang telah memperbaiki keamanannya

DAFTAR PUSTAKA

https://timesindonesia.co.id/indonesia-positif/385233/bagaimana-cara-memastikan-keamanan-cyber-saat-menggunakan-wifi-publik
https://www.cnbcindonesia.com/tech/20221122123049-37-390150/warga-ri-ini-cara-amankan-akun-internet-dari-maling-digital
https://www.wallblock.co.id/mengapa-antivirus-sangat-penting-bagi-keamanan-komputer-anda/
https://biztech.proxsisgroup.com/5-komponen-utama-security-operation-center-soc-strategi-organisasi-bertahan-lama/
https://www.hostnic.id/blog/berita/teknologi/penyebab-malware-mengenal-ancaman-dan-cara-mengatasinya/
https://www.batumenyan.desa.id/serangan-siber-terbaru-ancaman-dan-dampaknya-dalam-keamanan-digital/
https://www.biznetgio.com/news/apa-itu-cybersecurity
https://www.cloudeka.id/id/berita/web-sec/cara-menjaga-keamanan-jaringan-komputer/