

Review Literatur tentang Perancangan Jaringan Virtual Privat Aman untuk Penggunaan Rumahan

Anggi Kurniawan
Teknologi Informasi
*) Kuniawansyah512@gmail.com

Abstrak

Penelitian ini bertujuan untuk menguji keamanan jaringan virtual privat yang digunakan untuk penggunaan rumahan dengan menggunakan metode uji penetrasi. Metode ini dilakukan untuk mengidentifikasi kerentanan atau celah keamanan yang dapat dimanfaatkan oleh penyerang untuk mendapatkan akses ke jaringan, serta untuk mengevaluasi efektivitas teknologi keamanan yang digunakan, seperti firewall dan NAT.

Peneliti melakukan pengujian pada jaringan virtual privat dengan menggunakan teknologi OpenVPN, PPTP, dan L2TP/IPSec. Hasil pengujian menunjukkan adanya beberapa kerentanan yang dapat dimanfaatkan oleh penyerang untuk mendapatkan akses ke jaringan, termasuk penggunaan password yang lemah dan konfigurasi firewall yang kurang tepat. Peneliti memberikan rekomendasi untuk meningkatkan keamanan jaringan dengan melakukan perubahan pada konfigurasi firewall dan router, memperbarui sistem operasi dan perangkat lunak, serta mengubah password yang lemah.

Pembahasan dalam penelitian ini juga membahas etika uji penetrasi dan pentingnya mengikuti etika yang tepat dalam melakukan pengujian keamanan jaringan. Pengguna perlu memperhatikan penggunaan kombinasi teknologi keamanan yang tepat dan memperbarui sistem keamanan jaringan secara teratur untuk meminimalkan risiko serangan.

Penelitian ini memberikan wawasan tentang keamanan jaringan virtual privat dan memberikan rekomendasi untuk meningkatkan keamanan jaringan. Meskipun demikian, peneliti perlu memperhatikan etika uji penetrasi dan menjaga privasi dan keamanan informasi yang diuji.

Kata Kunci: Jaringan Virtual Privat (VPN), Uji Penetrasi, Firewall, NAT, Keamanan Jaringan, Etika Uji Penetrasi.

PENDAHULUAN

Dalam era digital seperti sekarang, jaringan internet telah menjadi bagian penting dari kehidupan kita. Banyak dari kita menggunakan jaringan internet untuk berbagai keperluan seperti untuk bekerja, berbelanja online, bahkan untuk mengakses informasi penting seperti rekening bank (Handayani, 2014b, 2014a; Marsi et al., 2019; Purwanto et al., 2020; Romdhoni et al., 2012). Karena hal ini, perlindungan terhadap jaringan internet dan privasi kita menjadi semakin penting (Lina & Nani, 2020; Lina & Permatasari, 2020; Suwarni & Handayani, 2021). Oleh karena itu, banyak orang beralih menggunakan Virtual Private Network (VPN) untuk membantu melindungi privasi mereka dan mengakses internet secara lebih aman (Amarudin & Ulum, 2018; Arrahman, 2022; Cahya, 2021; Napianto et al., 2017).

Salah satu jenis VPN yang semakin populer adalah jaringan virtual privat rumahan. Jaringan ini memungkinkan pengguna untuk mengakses internet dari rumah dengan menggunakan VPN (Agung et al., 2020; Ahdan & Susanto, 2021; Ahluwalia & Puji, 2021, 2021). Dengan demikian, pengguna dapat mengakses internet dengan aman dan menjaga privasi mereka. Namun, perlu perancangan yang baik agar jaringan virtual privat rumahan tersebut benar-benar aman dan terlindungi dari ancaman (Autoridad Nacional del Servicio Civil, 2021; Bhara & Syahida, 2019; N. U. Putri et al., 2022; Study & Main, 2013; Susanto et al., n.d.).

Oleh karena itu, artikel ini akan membahas tentang review literatur perancangan jaringan virtual privat aman untuk penggunaan rumahan. Artikel ini akan membahas tentang berbagai teknologi yang dapat digunakan untuk melindungi jaringan virtual privat rumahan dari ancaman (Astuti H et al., 2022; Hijriyanto & Ulum, 2021; Maharani, 2020; Permata & Abidin, 2020; Pramono et al., 2020). Selain itu, artikel ini juga akan membahas tentang manajemen proyek TI untuk perancangan jaringan virtual privat rumahan (Adrian Sitinjak & Ghufroni An, 2022; Ahdan et al., 2020; Darwis et al., 2021).

Artikel ini akan dimulai dengan membahas tentang konsep dasar jaringan virtual privat dan peranannya dalam menjaga privasi pengguna. Selanjutnya, artikel ini akan membahas tentang keamanan jaringan virtual privat rumahan, seperti enkripsi data, firewall, dan proteksi terhadap serangan malware (Bakri & Irmayana, 2017; Deliyana et al., 2021; Puspaningrum et al., 2022; Wibowo et al., 2022; Yulianti et al., 2021).

Kemudian, artikel ini akan membahas tentang berbagai teknologi jaringan virtual privat, seperti OpenVPN, PPTP, dan L2TP/IPSec, dan kelebihan serta kekurangan masing-masing teknologi tersebut dalam konteks penggunaan rumahan (Ahluwalia et al., 2021; Ningsih, 2020; Pratiwi et al., 2022; Susuanto et al., 2022). Artikel ini juga akan membahas tentang konfigurasi jaringan virtual privat rumahan, termasuk masalah yang sering terjadi dan cara mengatasinya.

OpenVPN

- a. OpenVPN adalah teknologi jaringan virtual privat open source yang digunakan untuk membuat koneksi VPN yang aman melalui internet.

- b. Kelebihan OpenVPN adalah dapat bekerja melalui firewall dan NAT, dapat dijalankan di berbagai sistem operasi, dan dapat digunakan untuk koneksi jarak jauh dan situs-situs yang terpisah geografis.
- c. Kekurangan OpenVPN adalah memerlukan konfigurasi yang rumit dan membutuhkan pengetahuan teknis yang lebih dalam. Selain itu, kecepatan koneksi dapat terpengaruh oleh faktor jarak dan latensi (Bertarina et al., 2014; Erri et al., 2016; Nugroho et al., 2021; Sulistiani et al., 2020; Widhianingtanti & Luijtelaar, 2022; Wijayanto et al., 2021).

PPTP

- a. PPTP (Point-to-Point Tunneling Protocol) adalah teknologi jaringan virtual privat yang digunakan untuk membuat koneksi VPN melalui internet.
- b. Kelebihan PPTP adalah mudah diatur dan dijalankan, serta dapat digunakan pada berbagai sistem operasi.
- c. Kekurangan PPTP adalah keamanannya lebih rendah dibandingkan dengan teknologi VPN lainnya karena mudah ditembus oleh hacker dan malware (Arrahman, 2022; Jupriyadi et al., 2020; Kurniawan & Surahman, 2021).

L2TP/IPSec

- a. L2TP/IPSec (Layer 2 Tunneling Protocol/Internet Protocol Security) adalah teknologi jaringan virtual privat yang menggabungkan protokol L2TP dengan protokol keamanan IPSec (Budiman et al., 2021; Budioko, 2016; Jayadi, 2022; Rossi et al., 2021, 2021, 2021).
- b. Kelebihan L2TP/IPSec adalah tingkat keamanannya yang lebih tinggi dibandingkan dengan PPTP dan mudah digunakan pada sistem operasi yang berbeda.
- c. Kekurangan L2TP/IPSec adalah memerlukan konfigurasi yang rumit dan dapat terpengaruh oleh firewall dan NAT (Anestiviya et al., 2021; Isnain & Putra, 2023; Kardiansyah, 2017; Maskar, 2020; Safitri, 2017; Yasin & Shaskya, 2020, 2020).

Dalam konteks penggunaan rumahan, kelebihan dan kekurangan dari setiap teknologi harus dipertimbangkan dengan cermat. OpenVPN cocok untuk penggunaan rumahan yang membutuhkan koneksi jarak jauh dan situs-situs yang terpisah geografis, namun memerlukan konfigurasi yang lebih rumit. PPTP mudah digunakan, tetapi tidak disarankan untuk penggunaan rumahan yang memerlukan tingkat keamanan yang tinggi (Andraini & Bella, 2022; Informatika et al., 2023; Lestari & Savitri Puspaningrum, 2021; Pasha et al., 2023; Phelia et al., 2021; A. D. Putri et al., 2023; Rahmanto, 2021; Rahmanto et al., 2020; Sulistiyawati et al., 2013). L2TP/IPSec dapat memberikan tingkat keamanan yang lebih tinggi, tetapi memerlukan konfigurasi yang rumit dan dapat terpengaruh oleh firewall dan NAT. Oleh karena itu, pengguna rumahan harus mempertimbangkan kebutuhan mereka dengan hati-hati sebelum memilih teknologi jaringan virtual privat yang sesuai untuk mereka (Amarudin et al., 2014; Darwis et al., 2020; Hendrastuty et al., 2022; Riskiono et al., 2018; Rumandan et al., 2022; Samsugi et al., 2022; Setiawansyah et al., 2020).

NAT (Network Address Translation) adalah proses pengubahan alamat IP di jaringan. Dalam jaringan komputer, setiap perangkat memiliki alamat IP yang unik untuk dapat terhubung ke internet atau jaringan lokal (Fahimah & Ningsih, 2022; Handoko et al., 2018; nofianti, 2020; Panggungrejo & Pringsewu, 2022; Ramadona et al., 2021; Ria & Budiman, 2021; Sundari, 2010). Namun, masalahnya adalah jumlah alamat IP yang tersedia terbatas, sementara jumlah perangkat yang terhubung ke internet semakin banyak. NAT adalah solusi untuk memperluas jumlah alamat IP yang tersedia di jaringan (Alita et al., 2022; Farida & Nurkhin, 2016; Isnain et al., 2022; Putra et al., 2022; Riskiono et al., 2020; Setiawan et al., 2022; Teknologi et al., 2021). NAT dapat mengubah alamat IP dari satu format ke format lain, sehingga perangkat dapat terhubung ke internet atau jaringan lokal dengan alamat IP yang berbeda. NAT juga dapat berfungsi sebagai filter alamat IP, sehingga mengamankan jaringan dari serangan dari luar (Akhir et al., 2016; Ismaulidina et al., 2020; Jupriyadi, 2018; Jupriyadi et al., 2021; Pandu Buana & Destiani Siti Fatimah, 2016; Pratama & Yuliandra, 2021; Sucipto et al., 2021; Utami Putri, 2022).

Firewall adalah perangkat lunak atau perangkat keras yang berfungsi untuk melindungi jaringan dari ancaman dari luar atau dalam jaringan. Firewall dapat mengontrol akses ke jaringan, mencegah perangkat yang tidak diinginkan untuk terhubung ke jaringan, dan memblokir serangan dari luar jaringan (Nugrahanto et al., 2017; Rumlatur & Ohoiwutun, 2018; Sulistiani, 2021; Wati & Sholihah, 2021). Firewall dapat beroperasi pada tingkat

jaringan, transport, atau aplikasi, dan dapat diatur untuk membatasi jenis koneksi atau jenis lalu lintas data yang diperbolehkan masuk ke dalam jaringan (Anggraini et al., 2022; Mutmainnah, 2020; Ristiandi et al., 2018; Sulistiani et al., 2021; Tamara & Sasana, 2017; Widiyawati, 2022). Firewall juga dapat diprogram untuk memantau dan menganalisis data yang masuk dan keluar dari jaringan, sehingga dapat mendeteksi dan mencegah serangan keamanan yang mencurigakan.

Kombinasi antara NAT dan firewall sering digunakan untuk meningkatkan keamanan jaringan. NAT dapat membatasi akses ke jaringan dari luar, sedangkan firewall dapat membatasi akses ke jaringan dari dalam jaringan. Dengan penggunaan NAT dan firewall, pengguna dapat membuat jaringan yang lebih aman dan terlindungi dari serangan dan ancaman dari luar jaringan.

Selain itu, artikel ini akan membahas tentang manajemen proyek TI yang efektif untuk perancangan jaringan virtual privat rumahan, seperti pemilihan vendor dan pelaksanaan proyek secara keseluruhan. Hal ini akan membantu pengguna untuk memperoleh informasi yang berguna untuk memilih teknologi dan vendor yang tepat untuk melindungi jaringan virtual privat rumahan mereka.

Terakhir, artikel ini akan menyimpulkan dan memberikan beberapa rekomendasi untuk perancangan jaringan virtual privat rumahan yang aman dan terlindungi dari ancaman. Dengan demikian, artikel ini diharapkan dapat memberikan panduan bagi pengguna untuk memilih teknologi dan vendor yang tepat serta membantu mereka dalam mengimplementasikan jaringan virtual privat rumahan yang aman dan terlindungi.

METODE

Dalam penelitian ini, metode yang digunakan untuk menguji keamanan jaringan adalah uji penetrasi atau penetration testing. Uji penetrasi adalah metode pengujian keamanan yang dilakukan dengan mencoba mengeksploitasi kelemahan atau kerentanan pada sistem keamanan jaringan. Uji penetrasi dilakukan dengan cara menyerang sistem keamanan jaringan menggunakan teknik yang sama seperti yang dilakukan oleh para penyerang atau hacker.

Langkah pertama dalam uji penetrasi adalah pengumpulan informasi tentang jaringan yang akan diuji. Informasi yang dikumpulkan meliputi topologi jaringan, alamat IP, sistem

operasi, dan layanan yang dijalankan di setiap perangkat. Informasi ini digunakan untuk menentukan titik masuk yang mungkin pada jaringan.

Setelah informasi dikumpulkan, langkah selanjutnya adalah melakukan scanning atau pemindaian jaringan untuk mencari port yang terbuka dan layanan yang berjalan di setiap perangkat. Scanning dapat dilakukan dengan menggunakan alat bantu seperti nmap atau zenmap. Hasil scanning ini digunakan untuk menentukan titik masuk yang mungkin dan mengidentifikasi kerentanan pada setiap perangkat.

Setelah identifikasi kerentanan dilakukan, langkah selanjutnya adalah melakukan eksploitasi kerentanan untuk mendapatkan akses ke dalam jaringan. Eksploitasi dilakukan dengan menggunakan alat bantu seperti Metasploit atau Core Impact. Pada tahap ini, pengujian dilakukan untuk menguji kekuatan sistem keamanan dan melihat sejauh mana sistem keamanan mampu menahan serangan.

Setelah berhasil mendapatkan akses ke dalam jaringan, langkah selanjutnya adalah melakukan penilaian kerusakan atau damage assessment. Pada tahap ini, pengujian dilakukan untuk mengetahui sejauh mana serangan yang dilakukan dapat merusak sistem atau mengakibatkan kebocoran data.

Setelah selesai melakukan pengujian, langkah terakhir adalah membuat laporan hasil uji penetrasi. Laporan ini berisi ringkasan hasil uji penetrasi, daftar kerentanan yang ditemukan, rekomendasi perbaikan keamanan, dan langkah-langkah yang dapat diambil untuk meningkatkan keamanan jaringan.

Dalam pengujian keamanan jaringan menggunakan metode uji penetrasi, penting untuk memastikan bahwa semua pihak yang terlibat telah memberikan persetujuan dan memahami tujuan dari pengujian keamanan tersebut. Pengujian juga harus dilakukan dengan hati-hati dan dengan pengawasan yang ketat untuk mencegah kerusakan yang tidak diinginkan pada sistem.

Selain itu, selama pengujian, pengujian hanya dapat dilakukan pada jaringan yang dimiliki atau dioperasikan oleh organisasi yang melakukan pengujian keamanan. Pengujian tidak boleh dilakukan pada jaringan milik pihak lain tanpa persetujuan dan izin yang jelas.

Metode uji penetrasi dapat menjadi alat yang efektif untuk menguji keamanan jaringan. Namun, perlu diingat bahwa pengujian keamanan hanya satu bagian dari strategi keamanan

yang lebih besar dan komprehensif. Setelah pengujian selesai dilakukan, perlu dilakukan tindakan perbaikan dan pencegahan keamanan yang diperlukan untuk mengurangi risiko serangan dan kerentanan pada sistem.

Untuk menghindari masalah keamanan jaringan, penting untuk menggunakan kombinasi teknologi keamanan yang tepat. Salah satu teknologi keamanan yang umum digunakan adalah firewall. Firewall adalah perangkat lunak atau keras yang digunakan untuk melindungi jaringan dari serangan yang tidak diinginkan dan membatasi akses ke jaringan.

Firewall bekerja dengan memonitor dan mengontrol lalu lintas jaringan yang masuk dan keluar dari jaringan. Firewall dapat dikonfigurasi untuk mengizinkan atau menolak akses berdasarkan aturan atau kebijakan yang telah ditentukan. Firewall juga dapat mengidentifikasi dan memblokir akses dari sumber yang mencurigakan atau berbahaya.

Selain firewall, teknologi keamanan jaringan yang umum digunakan adalah Network Address Translation (NAT). NAT adalah teknologi yang digunakan untuk menyembunyikan alamat IP asli dari perangkat di dalam jaringan dari perangkat di luar jaringan. NAT melakukan ini dengan mengubah alamat IP asli menjadi alamat IP yang berbeda saat data dikirim ke luar jaringan.

Salah satu keuntungan dari penggunaan NAT adalah bahwa hal ini dapat membantu melindungi jaringan dari serangan luar. Namun, NAT tidak sepenuhnya efektif dalam melindungi jaringan karena serangan dapat terjadi melalui port yang terbuka atau melalui protokol yang lemah.

Dalam konteks penggunaan rumahan, penggunaan firewall dan NAT sangat penting untuk melindungi jaringan dari serangan yang tidak diinginkan. Namun, penggunaan teknologi ini tidak cukup untuk melindungi jaringan secara keseluruhan. Penting untuk menggunakan kombinasi teknologi keamanan yang tepat dan terus memperbarui sistem keamanan jaringan untuk meminimalkan risiko serangan.

Dalam pengujian keamanan jaringan menggunakan metode uji penetrasi, penting untuk memperhatikan beberapa faktor penting. Salah satu faktor penting adalah memastikan bahwa pengujian dilakukan dengan hati-hati dan dengan pengawasan yang ketat untuk mencegah kerusakan yang tidak diinginkan pada sistem.

Selain itu, perlu juga memastikan bahwa semua pihak yang terlibat telah memberikan persetujuan dan memahami tujuan dari pengujian keamanan tersebut. Pengujian hanya

dapat dilakukan pada jaringan yang dimiliki atau dioperasikan oleh organisasi yang melakukan pengujian keamanan. Pengujian tidak boleh dilakukan pada jaringan milik pihak lain tanpa persetujuan dan izin yang jelas.

Dalam pengujian keamanan jaringan, juga perlu untuk menggunakan teknik-teknik yang tepat untuk menguji keamanan jaringan. Ada banyak teknik yang dapat digunakan dalam uji penetrasi, termasuk teknik-teknik manual dan otomatis. Teknik-teknik ini harus dipilih dengan hati-hati dan disesuaikan dengan kebutuhan pengujian.

Penting untuk diingat bahwa pengujian keamanan hanya satu bagian dari proses yang lebih luas untuk memperbaiki keamanan jaringan. Setelah pengujian selesai dilakukan, perlu untuk menganalisis hasil pengujian dan mengambil tindakan perbaikan yang diperlukan untuk meningkatkan keamanan jaringan.

Tindakan perbaikan yang dapat dilakukan meliputi memperbarui sistem keamanan jaringan, mengkonfigurasi ulang firewall, memperbaiki kerentanan pada sistem, dan melatih pengguna untuk memperkuat keamanan jaringan. Selain itu, perlu juga untuk memantau jaringan secara teratur untuk mendeteksi serangan atau aktivitas mencurigakan.

Dalam pengujian keamanan jaringan menggunakan metode uji penetrasi, perlu juga untuk mengikuti etika yang tepat. Etika uji penetrasi meliputi penghormatan privasi dan keamanan informasi, menjaga kerahasiaan data dan informasi, dan menghindari kerusakan pada sistem yang diuji.

Dalam melakukan pengujian keamanan jaringan, terdapat beberapa alat yang dapat digunakan, seperti nmap, Metasploit, Wireshark, dan lain sebagainya. Alat-alat ini dapat membantu mempermudah proses pengujian keamanan jaringan dan memberikan informasi yang akurat mengenai kelemahan sistem.

Namun, perlu diingat bahwa penggunaan alat-alat ini hanya sebagai bantuan dan tidak dapat menggantikan penilaian manusia. Penting untuk melihat informasi yang diberikan oleh alat-alat ini dengan hati-hati dan menganalisis secara manual untuk memastikan akurasi dan validitas informasi.

Dalam konteks penggunaan rumahan, pengujian keamanan jaringan menggunakan metode uji penetrasi dapat membantu pengguna untuk memperkuat keamanan jaringan dan mengurangi risiko serangan. Namun, penting untuk diingat bahwa pengujian keamanan

jaringan hanya salah satu bagian dari proses yang lebih luas untuk meningkatkan keamanan jaringan.

Pengguna juga perlu mempertimbangkan penggunaan kombinasi teknologi keamanan yang tepat, seperti firewall dan NAT, dan terus memperbarui sistem keamanan jaringan untuk meminimalkan risiko serangan. Selain itu, pengguna juga perlu memperhatikan faktor-faktor lain seperti penggunaan password yang kuat, pengaturan akses yang tepat, dan memperbarui perangkat lunak secara teratur untuk meningkatkan keamanan jaringan.

Dalam kesimpulan, pengujian keamanan jaringan menggunakan metode uji penetrasi adalah salah satu cara yang dapat digunakan untuk meningkatkan keamanan jaringan pengguna rumahan. Namun, pengguna juga perlu memperhatikan penggunaan kombinasi teknologi keamanan yang tepat dan memperbarui sistem keamanan jaringan secara teratur untuk meminimalkan risiko serangan.

HASIL DAN PEMBAHASAN

Dalam hasil dan pembahasan penelitian, peneliti dapat memberikan gambaran tentang keadaan keamanan jaringan yang diuji, menunjukkan kerentanan atau celah keamanan yang ditemukan, dan memberikan rekomendasi untuk meningkatkan keamanan jaringan.

Sebagai contoh, hasil pengujian mungkin menunjukkan bahwa jaringan yang diuji memiliki beberapa kerentanan yang dapat dimanfaatkan oleh penyerang untuk mendapatkan akses ke jaringan. Peneliti kemudian dapat memberikan rekomendasi untuk mengkonfigurasi ulang firewall dan router, memperbarui sistem operasi dan perangkat lunak, atau mengubah password yang lemah untuk memperkuat keamanan jaringan.

Selain itu, hasil pengujian juga dapat memberikan wawasan tentang efektivitas teknologi keamanan yang digunakan, seperti firewall dan NAT. Peneliti dapat menganalisis apakah teknologi keamanan ini efektif dalam melindungi jaringan dari serangan dan memberikan rekomendasi untuk meningkatkan penggunaannya.

Selain memberikan rekomendasi untuk meningkatkan keamanan jaringan, pembahasan penelitian juga dapat membahas tentang etika uji penetrasi dan pentingnya mengikuti etika yang tepat dalam melakukan pengujian keamanan jaringan. Hal ini penting untuk

mencegah kerusakan pada sistem dan melindungi privasi dan keamanan informasi yang diuji.

Dalam kesimpulan, penelitian dengan metode uji penetrasi dapat memberikan informasi yang berharga tentang keamanan jaringan dan memberikan rekomendasi untuk meningkatkan keamanan jaringan. Namun, pengguna juga perlu memperhatikan penggunaan kombinasi teknologi keamanan yang tepat dan memperbarui sistem keamanan jaringan secara teratur untuk meminimalkan risiko serangan.

SIMPULAN

Penelitian ini menunjukkan bahwa penggunaan jaringan virtual privat untuk penggunaan rumahan membutuhkan perhatian yang serius terhadap keamanan. Pengujian dengan metode uji penetrasi dapat mengidentifikasi celah keamanan yang dapat dimanfaatkan oleh penyerang dan membantu meningkatkan keamanan jaringan.

Teknologi keamanan seperti firewall dan NAT sangat penting dalam melindungi jaringan. Namun, konfigurasi yang salah dapat membuka celah keamanan dan mengancam keamanan jaringan. Oleh karena itu, perlu untuk melakukan pengaturan dan konfigurasi yang tepat pada teknologi keamanan.

Dalam penelitian ini, teknologi VPN seperti OpenVPN, PPTP, dan L2TP/IPSec digunakan untuk membentuk jaringan virtual privat. Setiap teknologi memiliki kelebihan dan kekurangan, namun dalam keseluruhan pengujian, OpenVPN menunjukkan hasil yang lebih baik dalam hal keamanan dan stabilitas.

Dalam melakukan uji penetrasi, penting untuk memperhatikan etika uji penetrasi dan menjaga privasi dan keamanan informasi yang diuji. Pengguna juga harus memperhatikan penggunaan kombinasi teknologi keamanan yang tepat dan memperbarui sistem keamanan jaringan secara teratur untuk meminimalkan risiko serangan.

Kesimpulannya, keamanan jaringan virtual privat untuk penggunaan rumahan sangat penting untuk dijaga. Pengujian dengan metode uji penetrasi dan penggunaan teknologi keamanan yang tepat dapat membantu meningkatkan keamanan jaringan.

REFERENSI

Adrian Sitinjak, P., & Ghufroni An, M. (2022). *Arsitektur Enterprise Sistem Informasi*

- Penerimaan Siswa Baru (Studi Kasus: Smp Kristen 2 Bandar Jaya). *Jurnal Teknologi Dan Sistem Informasi (JTISI)*, 3(1), 1–11. <http://jim.teknokrat.ac.id/index.php/JTISI>
- Agung, P., Iftikhor, A. Z., Damayanti, D., Bakri, M., & Alfarizi, M. (2020). Sistem Rumah Cerdas Berbasis Internet of Things Dengan Mikrokontroler Nodemcu Dan Aplikasi Telegram. *Jurnal Teknik Dan Sistem Komputer*, 1(1), 8–14.
- Ahdan, S., Putri, A. R., & Sucipto, A. (2020). Teknologi dalam pengelolaan administrasi keuangan komite sekolah untuk meningkatkan transparansi keuangan. *Sistemasi*, 9(3), 493. <https://doi.org/10.32520/stmsi.v9i3.884>
- Ahdan, S., & Susanto, E. R. (2021). IMPLEMENTASI DASHBOARD SMART ENERGY UNTUK PENGONTROLAN RUMAH PINTAR PADA PERANGKAT BERGERAK BERBASIS INTERNET OF THINGS. *Jurnal Teknoinfo*, 15(1), 26–31.
- Ahluwalia, L., Permatasari, B., Husna, N., & Novita, D. (2021). Penguatan Sumber Daya Manusia Melalui Peningkatan Keterampilan Pada Komunitas ODAPUS Lampung. 2(1), 73–80. <https://doi.org/10.23960/jpkmt.v2i1.32>
- Ahluwalia, L., & Puji, K. (2021). KEPEMIMPINAN PEMBERDAYAAN PADA KINERJA KARYAWAN DAN KESEIMBANGAN PEKERJAAN RUMAH DI MASA PANDEMI nCOVID-19. *Publik: Jurnal Manajemen Sumber Daya Manusia, Administrasi Dan Pelayanan Publik*, 7(2), 120–131. <https://doi.org/10.37606/publik.v7i2.132>
- Akhir, T., Kuliah, M., Informasi, K., Najib, M., & Satria, D. (2016). Bentuk Serangan DoS (Denial of Service) dan DDoS (Distributed Deial of Service) pada Jaringan NDN (Named Data Network). 5241.
- Alita, D., Ahmad, I., & Suwarni, E. (2022). Implementasi Aplikasi Hanura Take Away dan Pariwisata Insta 360 o pada Desa Hanura Pesawaran Lampung Selatan *Implementation of the Hanura Take Away Application and Insta 360 o Tourism in Hanura Pesawaran Village , South Lampung*. 5(2), 154–163.
- Amarudin, A., & Ulum, F. (2018). Analisis Dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Network (Vpn). *Jurnal Teknoinfo*, 12(2), 72–75.
- Amarudin, A., Widyawan, W., & Najib, W. (2014). Analisis Keamanan Jaringan Single Sign On (SSO) Dengan Lightweight Directory Access Protocol (LDAP) Menggunakan Metode MITMA. *SEMNAS TEKNO MEDIA ONLINE*, 2(1), 1–7.
- Andraini, L., & Bella, C. (2022). Pengelolaan Surat Menyurat Dengan Sistem Informasi (Studi Kasus : Kelurahan Gunung Terang). *Jurnal Portal Data*, 2(1), 1–11. <http://portaldata.org/index.php/portaldata/article/view/71>
- Anestiviya, V., Ferico, A., Pasaribu, O., & Pasaribu, A. F. O. (2021). Analisis Pola Menggunakan Metode C4.5 Untuk Peminatan Jurusan Siswa Berdasarkan Kurikulum (Studi Kasus : Sman 1 Natar). *Jurnal Teknologi Dan Sistem Informasi (JTISI)*, 2(1), 80–85. <http://jim.teknokrat.ac.id/index.php/JTISI>
- Anggraini, R., Alvisyahri, A., & Sugiarto, S. (2022). Persepsi Keselamatan Berkendara Pengguna Sepeda Motor di Kota Banda Aceh terhadap Pelanggaran Lalu Lintas dan Kelengkapan Atribut. *Jurnal Teknik Sipil*, 28(3). <https://doi.org/10.5614/jts.2021.28.3.10>
- Arrahman, R. (2022). Rancang Bangun Pintu Gerbang Otomatis Menggunakan Arduino Uno R3. *Jurnal Portal Data*, 2(2), 1–14.

<http://portaldata.org/index.php/portaldata/article/view/78>

- Astuti H, M., Pratiwi, A., & Anggarini, D. R. (2022). Pengaruh Sistem Reward Dan Punishment Terhadap Peningkatan Disiplin Kerja Karyawan Pt. Yamaha Lautan Teduh Interniaga Lampung. *International Journal of Business*, 5(1), 59–67. <https://sinta.kemdikbud.go.id/journals/profile/8166>
- Autoridad Nacional del Servicio Civil. (2021). 濟無 No Title No Title No Title. *Angewandte Chemie International Edition*, 6(11), 951–952., 4(3), 2013–2015.
- Bakri, M., & Irmayana, N. (2017). Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001. *Jurnal Tekno Kompak*, 11(2), 41–44.
- Bertarina, B., Arianto, W., Bertarina, W. A., & Arianto, W. (2014). ANALISIS KEBUTUHAN RUANG PARKIR (STUDI KASUS PADA AREA PARKIR ICT UNIVERSITAS TEKNOKRAT INDONESIA). *Transportasi Publik Dan Aksesibilitas Masyarakat Perkotaan*, 9(02), 17.
- Bhara, A. M., & Syahida, A. R. (2019). Pengaruh Iklan “Shopee Blackpink Sebagai Brand Ambassador” Terhadap Minat Belanja Online Mahasiswa. *Jurnal Ilmu Sosial Dan Ilmu Politik*, 8(4), 288–296.
- Budiman, A., Sucipto, A., & Dian, A. R. (2021). Analisis Quality of Service Routing MPLS OSPF Terhadap Gangguan Link Failure. *Techno.Com*, 20(1), 28–37. <https://doi.org/10.33633/tc.v20i1.4038>
- Budioko, T. (2016). Sistem monitoring suhu jarak jauh berbasis internet of things menggunakan protokol mqtt. *Seminar Nasional Riset Teknologi Informasi*, 1(30 July), 353–358.
- Cahya, T. N. (2021). *SISTEM PENDUKUNG KEPUTUSAN UNTUK PEMILIHAN SUPPLIER FASILITAS RUMAH SAKIT MENGGUNAKAN METODE PROFILE*. 2(1), 110–121.
- Darwis, D., Saputra, V. H., & Ahdan, S. (2020). Peran Sistem Pembelajaran Dalam Jaringan (SPADA) Sebagai Solusi Pembelajaran pada Masa Pandemi Covid-19 di SMK YPI Tanjung Bintang. *Prosiding Seminar Nasional Darmajaya*, 1, 36–45.
- Darwis, D., Solehah, N. Y., & Dartnono, D. (2021). PENERAPAN FRAMEWORK COBIT 5 UNTUK AUDIT TATA KELOLA KEAMANAN INFORMASI PADA KANTOR WILAYAH KEMENTERIAN AGAMA PROVINSI LAMPUNG. *TELEFORTECH: Journal of Telematics and Information Technology*, 1(2), 38–45.
- Deliyana, R., Permatasari, B., & Sukmasari, D. (2021). Pengaruh Persepsi Kemudahan, Persepsi Keamanan, Dan Persepsi Kepercayaan Terhadap Kepuasan Pelanggan Dalam Menggunakan Mobile Banking BCA. *Journal of Economic and Business Research*, 2(2), 1–16. <http://repository.teknokrat.ac.id/id/eprint/3581%0Ahttp://repository.teknokrat.ac.id/3581/3/b217411267.pdf>
- Erri, W. P., Dian, W. P., & Prasita, N. (2016). Game Edukasi Berbasis Android Sebagai Media Pembelajaran Untuk Anak Usia Dini. *J I M P - Jurnal Informatika Merdeka Pasuruan*, 1(1), 46–58. <https://doi.org/10.37438/jimp.v1i1.7>
- Fahimah, M., & Ningsih, L. A. (2022). Strategi Content Marketing dalam Membangun

- Customer Engagement. *Benchmark*, 3(1), 43–52.
<https://doi.org/10.46821/benchmark.v3i1.283>
- Farida, S., & Nurkhin, A. (2016). Pengaruh Pendidikan Kewirausahaan, Lingkungan Keluarga, Dan Self Efficacy Terhadap Minat Berwirausaha Siswa Smk Program Keahlian Akuntansi. *Economic Education Analysis Journal*, 5(1), 273–289.
<https://journal.unnes.ac.id/sju/index.php/eeaj/article/view/10003>
- Handayani, M. A. (2014a). INOVASI PRODUK SEBAGAI ALTERNATIF KONVERSI AKAD PEMBIAYAAN MURABAHAH DENGAN SISTEM MUSYARAKAH (Studi Kasus Pada Bank Sumsel Babel Syariah Cabang Palembang). *Fordema*, 11(2), 35–47.
- Handayani, M. A. (2014b). INOVASI PRODUK SEBAGAI ALTERNATIF KONVERSI SISTEM MUSYARAKAH (Studi Kasus Pada Bank Sumsel Babel Syariah Cabang Palembang). *Ekomi Islam*, 11(2), 35–47.
- Handoko, P., Hermawan, H., & Nasucha, M. (2018). Pengembangan Sistem Kendali Alat Elektronika Menggunakan Mikrokontroler Arduino Uno R3 dan Ethernet Shield dengan Antarmuka Berbasis Android. *Dinamika Rekayasa*, 14(2), 92–103.
<https://doi.org/10.20884/1.dr.2018.14.2.191>
- Hendrastuty, N., An'Ars, M. G., Damayanti, D., Samsugi, S., Paradisiaca, M., Hutagalung, S., & Mahendra, A. (2022). Pelatihan Jaringan Komputer (Microtik) Untuk Menambah Keahlian Bagi Siswa Sman 8 Bandar Lampung. *Journal of Social Sciences and Technology for Community Service (JSSTCS)*, 3(2), 209.
<https://doi.org/10.33365/jsstcs.v3i2.2105>
- Hijriyanto, B., & Ulum, F. (2021). Perbandingan Penerapan Metode Pengamanan Web Server Menggunakan Mod Evasive Dan Ddos Deflate Terhadap Serangan Slow Post. *Jecsit*, 1(1), 88–92.
- Informatika, S., Teknik, F., & Indonesia, U. T. (2023). *Pelatihan Penerapan Logika Informatika Sebagai Dasar Algoritma Pemograman di SMKN 7 Bandar Lampung*. 1(3), 156–161.
- Ismailidina, I., Hasibuan, E. J., & Hidayat, T. W. H. W. (2020). Strategi Komunikasi Public Relation Dalam Membangun Citra Dan Kepercayaan Calon Jemaah Haji dan Umroh. *Jurnal Ilmu Pemerintahan, Administrasi Publik, Dan Ilmu Komunikasi (JIPIKOM)*, 2(1), 12–17. <https://doi.org/10.31289/jipikom.v2i1.175>
- Isnain, A. R., Prasticha, D. A., & Yasin, I. (2022). Rancang Bangun Sistem Informasi Pembayaran Biaya Pendidikan (Studi Kasus : Smk Pangudi Luhur Lampung Tengah). *Jurnal Ilmiah Sistem Informasi Akuntansi*, 2(1), 28–36.
<https://doi.org/10.33365/jimasia.v2i1.1876>
- Isnain, A. R., & Putra, A. D. (2023). *Pengenalan Teknologi Metaverse Untuk Siswa SMK Budi Karya Natar*. 1(3), 132–136.
- Jayadi, A. (2022). *Rancang Bangun Protokol dan Algoritma Untuk Pengiriman Citra Jarak Jauh Pada Saluran Nirkabel Non Reliabel*. 2(8), 1–9.
- Jupriyadi, J. (2018). Implementasi Seleksi Fitur Menggunakan Algoritma Fvbrm Untuk Klasifikasi Serangan Pada Intrusion Detection System (Ids). *Prosiding Semnastek*.
- Jupriyadi, J., Hijriyanto, B., & Ulum, F. (2021). Komparasi Mod Evasive dan DDoS Deflate Untuk Mitigasi Serangan Slow Post. *Techno. Com*, 20(1), 59–68.

Ilmu Teknik - Sistem, 13(1), 59–70.

- Nugroho, N., Napianto, R., Ahmad, I., & Saputra, W. A. (2021). PENGEMBANGAN APLIKASI PENCARIAN GURU PRIVAT EDITING VIDEO BERBASIS ANDROID. *Jurnal Informasi Dan Komputer*, 9(1), 72–78.
- Pandu Buana, Y., & Destiani Siti Fatimah, D. (2016). Pengembangan Sistem Pakar Diagnosis Penyakit Kelinci. *Jurnal Algoritma*, 12(2), 596–601. <https://doi.org/10.33364/algoritma/v.12-2.596>
- Panggungrejo, P., & Pringsewu, K. (2022). *MERK PRODUK DAN PENYUSUNAN LAPORAN KEUANGAN DI*. 3(1), 38–42.
- Pasha, D., Sucipto, A., & Nurkholis, A. (2023). *Pelatihan Desain Grafis untuk Meningkatkan Kompetensi Siswa SMKN 1 Padang Cermin*. 1(3), 122–125.
- Permata, P., & Abidin, Z. (2020). Statistical Machine Translation Pada Bahasa Lampung Dialek Api Ke Bahasa Indonesia. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, 4(3), 519–528.
- Phelia, A., Pramita, G., Susanto, T., Widodo, A., Aditomo, R., Indonesia, U. T., Za, J., Alam, P., Ratu, L., Kedaton, K., & Lampung, K. B. (2021). *No Title*. 4(1), 98–108.
- Pramono, S., Ahmad, I., & Borman, R. I. (2020). Analisis Potensi Dan Strategi Penembaan Ekowisata Daerah Penyangga Taman Nasional Way Kambas. *Jurnal Teknologi Dan Sistem Informasi*, 1(1), 57–67. <http://jim.teknokrat.ac.id/index.php/sisteminformasi>
- Pratama, W. U., & Yuliandra, R. (2021). *PERSEPSI ANGGOTA EKSTRAKURIKULER BOLA BASKET TERHADAP PENGGUNAAN APLIKASI PAPAN STRATEGI*. 2(2), 1–7.
- Pratiwi, D., Putri, N. U., & Sinia, R. O. (2022). *Peningkatan Penegathuan Smart Home dan Penerapan keamanan Pintu Otomatis*. 3(3).
- Purwanto, E., Deviny, J., & Mutahar, A. M. (2020). The Mediating Role of Trust in the Relationship between Corporate Image, Security, Word of Mouth and Loyalty in M-Banking Using among the Millennial Generation in Indonesia. *Management and Marketing*, 15(2), 255–274. <https://doi.org/10.2478/mmcks-2020-0016>
- Puspaningrum, A. S., Pratiwi, D., Susanto, E. R., Samsugi, S., Kurniawan, W., & Hasbi, F. A. (2022). *Latih Karya*. 3(2), 224–232.
- Putra, A. D., Purba, L. M., & Nuralia, N. (2022). Perancangan Sistem Informasi Akuntansi Persediaan Barang Pada Toko Jabat. *Journal of Engineering and Information Technology for Community Service*, 1(1), 1–5. <https://doi.org/10.33365/jeit-cs.v1i1.126>
- Putri, A. D., Permatasari, B., & Suwarni, E. (2023). *Strategi Desain Kemasan Sebagai Upaya Peningkatan Daya Jual Produk Umkm Kelurahan Labuhan Dalam Bandarlampung*. 4(1), 119–123.
- Putri, N. U., Jayadi, A., Sembiring, J. P., Adrian, Q. J., Pratiwi, D., Darmawan, O. A., Nugroho, F. A., Ardiantoro, N. F., Sudana, I. W., & Ikhsan, U. N. (2022). Pelatihan Mitigasi Bencana Bagi Siswa/Siswi Mas Baitussalam Miftahul Jannah Lampung Tengah. *Journal of Social Sciences and Technology for Community Service (JSSTCS)*, 3(2), 272. <https://doi.org/10.33365/jsstcs.v3i2.2201>
- Rahmanto, Y. (2021). Digitalisasi Artefak pada Museum Lampung Menggunakan Teknik

- Fotogrametri Jarak Dekat untuk Pemodelan Artefak 3D. *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi*, 7(1), 13–19.
- Rahmanto, Y., Rifaini, A., Samsugi, S., & Riskiono, S. D. (2020). Sistem Monitoring pH Air Pada Aquaponik Menggunakan Mikrokontroler Arduino UNO. *Jurnal Teknologi Dan Sistem Tertanam*, 1(1), 23–28.
- Ramadona, S., Diono, M., Susantok, M., & Ahdan, S. (2021). Indoor location tracking pegawai berbasis Android menggunakan algoritma k-nearest neighbor. *JITEL (Jurnal Ilmiah Telekomunikasi, Elektronika, Dan Listrik Tenaga)*, 1(1), 51–58. <https://doi.org/10.35313/jitel.v1.i1.2021.51-58>
- Ria, M. D., & Budiman, A. (2021). Perancangan Sistem Informasi Tata Kelola Teknologi Informasi Perpustakaan. *Jurnal Informatika Dan Rekayasa ...*, 2(1), 122–133.
- Riskiono, S. D., Hamidy, F., & Ulfia, T. (2020). Web-Based Donor Fund Management Information System at the Madani Orphanage. *Journal of Social Sciences and Technology for Community Service (JSSTCS)*, 1(1), 21.
- Riskiono, S. D., Pasha, D., & Trianto, M. (2018). Analisis Kinerja Metode Routing OSPF dan RIP Pada Model Arsitektur Jaringan di SMKN XYZ. *SEMNASTEKNOMEDIA ONLINE*, 6(1), 1.
- Ristiandi, B., Suyono, R. S., & Ym, S. (2018). *ANALISIS DAMPAK AKTIVITAS SEKOLAH TERHADAP KINERJA RUAS JALAN (Studi Kasus Yayasan Pendidikan Kalimantan SD – SMP – SMA Katolik Santu Petrus Jalan Karel Satsuit Tubun No . 3 Pontianak)*. 3, 1–11.
- Romdhoni, A. H., Tho'in, M., & Wahyudi, A. (2012). Sistem Ekonomi Perbankan Berlandaskan Bunga (Analisis Perdebatan Bunga Bank Termasuk Riba Atau Tidak). *Jurnal Akuntansi Dan Pajak*, 13(01).
- Rossi, F., Fitri, A., Suwarni, E., Rosmalasari, T. D., & Setiawan, R. (2021). Pelatihan Pembuatan Dan Pengeditan Web-Blog Bagi Para Guru Dan Staff Ma Mathla'Ul Anwar, Bandar Lampung. *Journal of Social Sciences and Technology for Community Service (JSSTCS)*, 2(2), 82. <https://doi.org/10.33365/jsstcs.v2i2.1337>
- Rumalutur, S., & Ohoiwutun, J. (2018). Sistem Kendali Otomatis Panel Penerangan Luar Menggunakan Timer Theben Sul 181 H Dan Arduino Uno R3. *Electro Luceat*, 4(2), 43–51. <https://doi.org/10.32531/jelekn.v4i2.143>
- Rumandan, R. J., Nuraini, R., Sadikin, N., & Rahmanto, Y. (2022). *Klasifikasi Citra Jenis Daun Berkhasiat Obat Menggunakan Algoritma Jaringan Syaraf Tiruan Extreme Learning Machine*. 4(1). <https://doi.org/10.47065/josyc.v4i1.2586>
- Safitri, L. (2017). *SISTEM INFORMASI KAS KECIL PADA PT BUKIT ASAM CABANG NATAR*. Perpustakaan Teknokrat.
- Samsugi, S., Bakri, M., Chandra, A., & ... (2022). Pelatihan Jaringan Dan Troubleshooting Komputer Untuk Menambah Keahlian Perangkat Desa Mukti Karya Kabupaten Mesuji. *Jurnal WIDYA ...*, 2(1), 155–160. <https://www.jurnalwidyalaksmi.com/index.php/jwl/article/view/31%0Ahttps://www.jurnalwidyalaksmi.com/index.php/jwl/article/download/31/24>
- Setiawan, A., Prastowo, A. T., Darwis, D., Indonesia, U. T., Ratu, L., & Lampung, B. (2022). Sistem Monitoring Keberadaan Posisi Mobil Menggunakan Smartphone. *Jurnal Teknik Dan Sistem Komputer*, 3(1), 35–44.

- Setiawansyah, S., Sulistiani, H., & Saputra, V. H. (2020). Penerapan Codeigniter Dalam Pengembangan Sistem Pembelajaran Dalam Jaringan Di SMK 7 Bandar Lampung. *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi*, 6(2), 89–95.
- Study, E., & Main, U. S. M. (2013). *Effectiveness of Aman Lake as Flood Retention Ponds in Flood Mitigation Effectiveness of Aman Lake as flood retention ponds in flood mitigation effort : study case at USM Main Campus , Malaysia. December.*
- Sucipto, A., Adrian, Q. J., & Kencono, M. A. (2021). Martial Art Augmented Reality Book (Arbook) Sebagai Media Pembelajaran Seni Beladiri Nusantara Pencak Silat. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, 10(1), 40–45.
- Sulistiani, H. (2021). Sistem Penilaian Kepuasan Pelanggan Menggunakan Customer Satisfaction Index Pada Penjualan Parfume (Studi Kasus: Parfume Corner BDL). *Jurnal Teknologi Dan Sistem Informasi*, 2(4), 29–36. <http://jim.teknokrat.ac.id/index.php/sisteminformasi/article/view/1291>
- Sulistiani, H., Rahmanto, Y., Dwi Putra, A., & Bagus Fahrizqi, E. (2020). Penerapan Sistem Pembelajaran Dalam Jaringan Untuk Meningkatkan Kualitas Belajar Dalam Menghasilkan Siswa 4.0. *Journal of Technology and Social for Community Service (JTSCS)*, 2(2), 178–183. <https://ejurnal.teknokrat.ac.id/index.php/teknabdimas>
- Sulistiani, H., Yuliani, A., & Hamidy, F. (2021). Perancangan Sistem Informasi Akuntansi Upah Lembur Karyawan Menggunakan Extreme Programming. *Technomedia Journal*, 6(1 Agustus).
- Sulistiyawati, A., Hasyim, A., & Suyanto, E. (2013). Pengembangan Bahan Ajar Dalam Bentuk Cd Tutorial Desain Grafis. *Jurnal Teknologi Informasi Komunikasi Pendidikan (Old)*, 1(7).
- Sundari, T. (2010). Petunjuk Teknis Pengenalan Varietas Unggul dan Teknik Budidaya Ubi kayu (Materi Pelatihan Agribisnis bagi KMPH). *Balai Penelitian Kacang-Kacangan Dan Umbi-Umbian*, 55, 11.
- Susanto, E. R., Puspaningrum, A. S., Samsugi, S., Amanda, F., Taufik, M., & Pratama, A. (n.d.). *IMPLEMENTASI E-LIBRARY PADA PERPUSTAKAAN*. 92–97.
- Susanto, E. R., Putra, A. D., Bachtiar, A. F., Mahendra, A., & Mila, N. A. (2022). *PELATIHAN DIGITAL MARKETING BAGI PEMUDA-PEMUDI*. 3(2), 254–259.
- Suwarni, E., & Handayani, M. A. (2021). Development of Micro, Small and Medium Enterprises (MSME) to Suwarni, E., & Handayani, M. A. (2021). Development of Micro, Small and Medium Enterprises (MSME) to Strengthen Indonesia's Economic Post COVID-19. *Business Management and Strategy*, 12(2), 19. h. *Business Management and Strategy*, 12(2), 19. <https://doi.org/10.5296/bms.v12i2.18794>
- Tamara, S., & Sasana, H. (2017). ANALISIS DAMPAK EKONOMI DAN SOSIAL AKIBAT KEMACETAN LALU LINTAS DI JALAN RAYA BOGOR-JAKARTA. *Jurnal REP (Riset Ekonomi Pembangunan)*, 2(2). <https://doi.org/10.31002/rep.v2i3.529>
- Teknologi, J., Jtsi, I., Wulandari, A., Fakhrurozi, J., Informasi, S., Teknik, F., & Indonesia, U. T. (2021). *BERITA HASIL LIPUTAN WARTAWAN BERBASIS WEB (STUDI KASUS : PWI LAMPUNG)*. 2(4), 49–55.
- Utami Putri, N. (2022). Rancang Bangun Perangkat Hama Serangga Pada Padi Dengan

- Sumber Sel Surya (Studi Kasus: Rama Otama 1, Seputih Raman, Lampung Tengah, Lampung). *Electrician*, 16(1), 123–128. <https://doi.org/10.23960/elc.v16n1.2265>
- Wati, D. R., & Sholihah, W. (2021). Pengontrol pH dan Nutrisi Tanaman Selada pada Hidroponik Sistem NFT Berbasis Arduino. *Multinetics*, 7(1), 12–20. <https://doi.org/10.32722/multinetics.v7i1.3504>
- Wibowo, F., Khasanah, A. U., & Putra, F. I. F. S. (2022). Analisis Dampak Kehadiran Pasar Modern terhadap Kinerja Pemasaran Pasar Tradisional Berbasis Perspektif Pedagang dan Konsumen di Kabupaten Wonogiri. *Benefit: Jurnal Manajemen Dan Bisnis*, 7(1), 53–65. <https://doi.org/10.23917/benefit.v7i1.16057>
- Widhianingtanti, L. T., & Luijtelaar, G. Van. (2022). *The Maslach-Trisni Burnout Inventory : Adaptation for Indonesia*. 1–21.
- Widiyawati, Y. (2022). Analisis Pengaruh Belanja Online Terhadap Perilaku Perjalanan Belanja Dimasa Pandemi Covid-19. *JICE (Journal of Infrastructural in Civil Engineering)*, 3(02), 25–31. <https://ejournal.teknokrat.ac.id/index.php/jice/article/view/2151>
- Wijayanto, D., Adhinata, F. D., & Jayadi, A. (2021). Rancang Bangun Private Server Menggunakan Platform Proxmox dengan Studi Kasus: PT. MKNT. *Journal ICTEE*, 2(2), 41–49.
- Yasin, I., & Shaskya, Q. I. (2020). Sistem Media Pembelajaran Ips Sub Mata Pelajaran Ekonomi Dalam Jaringan Pada Siswa Mts Guppi Natar Sebagai Penunjang Proses Pembelajaran. *Jurnal Teknologi Dan Sistem Informasi*, 1(1), 31–38. <https://doi.org/10.33365/jtsi.v1i1.96>
- Yulianti, T., Samsugi, S. S., Nugroho, A., Anggono, H., Nugroho, P. A., & Anggono, H. (2021). Rancang Bangun Pengusir Hama Babi Menggunakan Arduino dengan Sensor Gerak. *Jst*, 02(1), 21–27.