ZONAsi Jurnal Sistem Informasi
ZONAsi VOL. 7 NO. 3 Sep 2025
Page: 1103 - 1114
ISSN: 2656-7407 (Online)
2656-7393 (Print)

PENERAPAN VPN *WIREGUARD* UNTUK KEAMANAN SERVER JARINGAN SAHABAT NET DARI SNIFFING ATTACK

Linna Oktaviana Sari[1], Reza Pahlevi[2], Ery Safrianti[3], R.A Rizka Qori Yuliana Putri[4]
[1,2,3,4]Jurusan Teknik Elektro, Program Studi Teknik Informatika, Fakultas Teknik, Universitas Riau,
Kampus Bina Widya, KM. 12,5 Simpang Baru, Pekanbaru, Riau, Indonesia,
Telp: 0761-63272/Fax: 0761-566821
e-mail: [1]linnaoasari@lecturer.unri.ac.id, [2]reza.pahlevi4559 @student.unri.ac.id,
[3]esafrianti@eng.unri.ac.id, [4]rizkaqoriyulianiputri@lecturer.unri.ac.id

Abstrak

Dalam era digital yang terus berkembang, kebutuhan akan sistem keamanan jaringan yang andal menjadi sangat penting, khususnya bagi penyedia layanan internet seperti Sahabat Net. Penelitian ini bertujuan meningkatkan keamanan jaringan dengan menerapkan protokol Virtual Private Network (VPN) WireGuard pada infrastruktur Sahabat Net yang sebelumnya rentan terhadap serangan sniffing. Metode yang digunakan adalah kualitatif deskriptif melalui observasi, wawancara, studi literatur, dan pengujian jaringan sebelum dan sesudah penerapan VPN. Pengujian awal menunjukkan bahwa jaringan tanpa enkripsi memungkinkan pencurian data sensitif pengguna melalui sniffing menggunakan Ettercap dan Wireshark. Setelah implementasi WireGuard VPN pada router Mikrotik, konfigurasi dan pengujian ulang membuktikan bahwa lalu lintas jaringan berhasil dienkripsi dan tidak lagi dapat diakses pihak ketiga. Hasil penelitian menunjukkan peningkatan signifikan dalam keamanan jaringan. Kesimpulannya, penerapan WireGuard VPN efektif dalam mencegah penyadapan data serta menjaga kerahasiaan dan integritas komunikasi jaringan di lingkungan Sahabat Net.
Kata kunci: *VPN, Wireguard, Sniffing, Enkripsi, Mikrotik.*

Abstract

In today's rapidly evolving digital era, the need for reliable network security systems is increasingly critical, especially for internet service providers such as Sahabat Net. This study aims to enhance network security by implementing the WireGuard Virtual Private Network (VPN) protocol on Sahabat Net's infrastructure, which was previously vulnerable to sniffing attacks. A descriptive qualitative method was applied through direct observation, interviews, literature review, and network testing before and after the VPN implementation. Initial tests revealed that, without encryption, sensitive user data could be intercepted using sniffing tools like Ettercap and Wireshark. After deploying WireGuard VPN on a Mikrotik router, network traffic was successfully encrypted, preventing third parties from accessing the data. The results show a significant improvement in network security. In conclusion, the implementation of WireGuard VPN proves effective in preventing data interception and ensuring the confidentiality and integrity of communications within Sahabat Net's network.
Keywords: *VPN, Wireguard, Sniffing, Encription, Mikrotik.*

1. PENDAHULUAN

Dalam era digital saat ini, internet telah menjadi komponen esensial dalam kehidupan masyarakat modern. Kemudahan dan ketersediaan akses terhadap jaringan internet telah mendorong transformasi dalam berbagai aktivitas manusia, mulai dari cara berinteraksi, bekerja, hingga proses pembelajaran dan kegiatan sehari-hari. Peran internet sangat signifikan, tidak hanya di wilayah perkotaan, tetapi juga menjangkau daerah pedesaan, sehingga turut memengaruhi perkembangan sosial dan ekonomi masyarakat secara luas.

Infrastruktur jaringan internet memainkan peran krusial dalam mendukung perkembangan era digital yang terus mengalami percepatan dan perubahan dinamis. Keberadaan internet tidak hanya merevolusi pola komunikasi antarindividu, tetapi juga menjadi katalisator transformasi di berbagai sektor strategis,

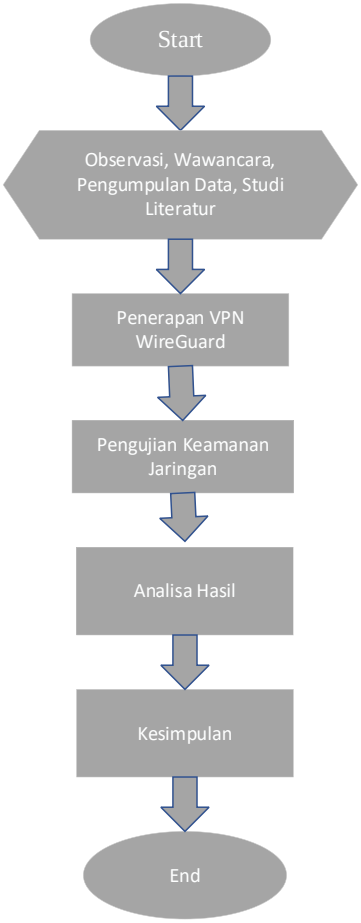
termasuk pendidikan, ekonomi dan bisnis, pemerintahan, serta pelayanan publik[1]. Penyedia layanan internet (ISP) dalam menyediankan layanan internet ke masyarakat memiliki berbagai atribut kualitas, seperti *jitter* dan sistem keamanan, yang memengaruhi daya saing mereka[2]. Kemajuan teknologi turut mendorong meluasnya kejahatan siber dalam jaringan, sehingga sistem keamanan jaringan memiliki peran penting dalam upaya pencegahan terhadap berbagai serangan yang dilakukan oleh pihak yang tidak bertanggung jawab[3]. Perlindungan data pribadi kini menjadi isu yang semakin krusial seiring dengan pesatnya perkembangan teknologi dan meningkatnya penggunaan internet. Banyak pengguna belum sepenuhnya menyadari risiko yang muncul, khususnya saat mengakses internet. Salah satu solusi yang dapat diterapkan untuk keamanan jaringan adalah penggunaan *Virtual Private Network*(VPN), karena VPN menjaga keamanan jaringan dengan membentuk terowongan virtual yang memungkinkan koneksi aman antara jaringan internal dan jaringan eksternal melalui internet[4]

Penelitian VPN pada jaringan internet banyak telah dilakukan. Penelitian pada [5] mengevaluasi potensi *WireGuard* protokol VPN modern sebagai solusi keamanan yang efisien untuk sistem IoT dengan keterbatasan sumber daya. Analisis menyeluruh juga dilakukan terhadap aspek keamanan VPN, meliputi perbandingan berbagai protokol enkripsi, kebijakan pencatatan data dan privasi, potensi kerentanan serta jenis serangan, hingga pentingnya pemilihan penyedia layanan VPN yang tepat telah dilakukan [6]. Analisis QoS (*delay, jitter, throughput, packet loss*) pada VoIP dengan VPN L2TP/IPSec dan *WireGuard* telah dilakukan[7]. Penelitian yang dilakukan [8] menguji protokol VPN modern, WireGuard, yang dikenal aman dan memiliki performa tinggi. Pengujian dilakukan pada topologi dua jaringan lokal (server dan klien) yang terhubung melalui internet. Penelitian pada [9] ini membahas perbandingan antara dua alat VPN dalam lingkungan hybrid-cloud, yaitu WireGuard sebagai solusi open-source dan Cloud VPN dari *Google Cloud Platform* (GCP) sebagai solusi tingkat enterprise. Evaluasi pada penelitian yang dilakukan [10] menunjukkan bahwa penggunaan VPN meningkatkan tingkat keamanan sekitar 65%, namun menurunkan performa jaringan sekitar 22%. Meski demikian, teknologi VPN modern seperti WireGuard dan IKEv2 terbukti mampu meminimalkan dampak negatif tersebut. Implementasi VPN berbasis L2TP pada Mikrotik untuk akses jarak jauh aman bagi admin jaringan sekolah. Koneksi publik diatur aman melalui protokol VPN telah dilakukan[11].Evaluasi penggunaan VPN untuk melindungi data dari sniffing. Hasil menunjukkan data sebelum terenkripsi dapat terlihat oleh Wireshark, sedangkan setelah tunneling VPN, data terenkripsi dan tidak bisa dibaca telah dilakukan[12]. Pada [13] telah dilakukan perancangan dengan simulasi topologi jaringan yang mendukung pengalamatan IPv6 serta konfigurasi VPN untuk mengamankan komunikasi antar jaringan. Hasil pengujian menunjukkan bahwa integrasi VPN dan IPv6 mampu meningkatkan efisiensi dalam pengalamatan serta memberikan tingkat keamanan yang memadai untuk transmisi data lintas jaringan.

Sahabat Net merupakan salah satu perusahaan penyedia layanan internet RT/RW di kota Perawang, dengan jumlah pelanggan sebanyak 183 pengguna. Meskipun telah memiliki infrastruktur jaringan yang menghubungkan pengguna di wilayah tersebut, perusahaan ini belum menerapkan sistem keamanan jaringan yang memadai. Akibatnya, akses jaringan masih dapat dilihat dan dimanfaatkan oleh pihak yang tidak berwenang. Ketidakhadiran mekanisme keamanan ini memungkinkan terjadinya peretasan dan penyadapan terhadap perangkat jaringan, terutama di ruang server, karena komunikasi dilakukan melalui jaringan publik tanpa enkripsi yang layak. Hal ini sangat berisiko mengingat terdapat data penting pelanggan yang harus dilindungi. Kebocoran data berpotensi menimbulkan kerugian besar bagi Sahabat Net, mulai dari kerusakan reputasi, hilangnya kepercayaan pelanggan. Bahkan, pencurian informasi strategis oleh pesaing bisa berdampak pada hilangnya keunggulan kompetitif dan pangsa pasar. Oleh karena itu, implementasi sistem keamanan jaringan yang kuat dan efisien menjadi kebutuhan mendesak. Untuk mengatasi permasalahan yang dihadapi Sahabat Net maka pada penelitian ini digunakan teknologi VPN dengan menggunakan protokol WireGuard. Salah satu layanan VPN yang tersedia pada perangkat MikroTik adalah WireGuard VPN. WireGuard merupakan jenis VPN yang dirancang dengan kesederhanaan, namun tetap menawarkan kecepatan, keamanan, dan teknologi yang modern. Saat ini, WireGuard telah mendukung berbagai platform seperti Linux, Windows, macOS, BSD, iOS, dan Android [14].

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif, yang berfokus pada analisis mendalam dan deskriptif. Metode kualitatif digunakan untuk menggali dan memahami fenomena yang terjadi secara alami, dengan fokus utama pada pendeskripsian, penafsiran, serta pemahaman yang mendalam terhadap makna subjektif dari pengalaman yang diteliti. Pengumpulan data dilakukan melalui teknik seperti wawancara, observasi, maupun telaah dokumen[15]. Proses penelitian diawali dengan tahap observasi dan wawancara, dilanjutkan dengan pengumpulan data dan informasi yang relevan, studi literatur, pengukuran terhadap jaringan yang sudah ada, konfigurasi sistem, hingga pengujian ulang terhadap sistem keamanan jaringan. Seluruh tahapan ini bertujuan untuk memperoleh gambaran menyeluruh mengenai kondisi dan keamanan jaringan. Adapun langkah-langkah kerja penelitian dirangkum dalam diagram alur metode penelitian yang ditampilkan pada gambar 1.



Gambar 1. Flowchart Metode Penelitian

2.1. Observasi, Wawancara dan Pengumpulan Data

Pada tahap observasi, telah dilakukan kunjungan langsung ke lokasi penelitian, yaitu Sahabat Net. Tujuan dari observasi ini adalah untuk mengenali dan menganalisis permasalahan jaringan yang sedang berlangsung di lokasi tersebut. Di ruang server, terdapat sejumlah perangkat yang saling terhubung dalam jaringan Sahabat Net, di antaranya Access Point, router Mikrotik, modem, dan perangkat OLT.

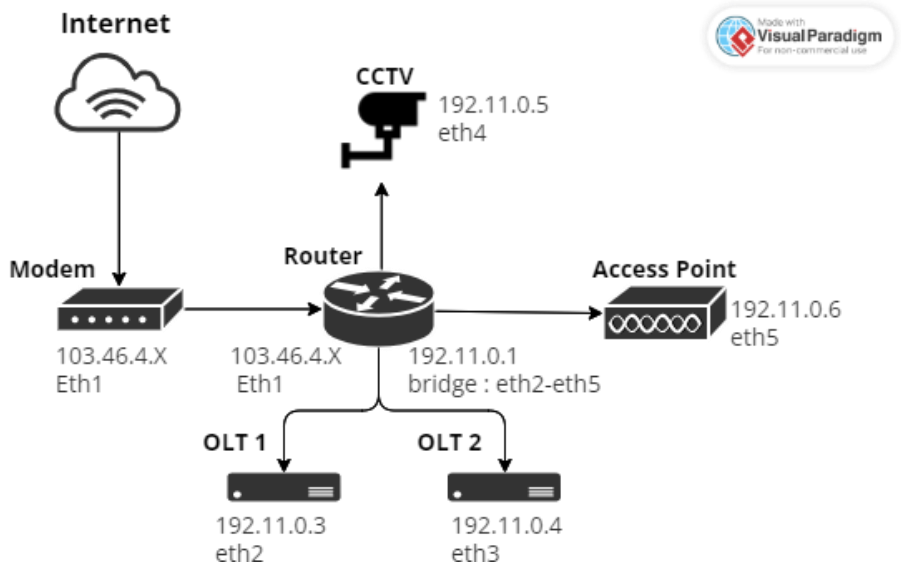
Access Point berfungsi sebagai penghubung utama antara pelanggan dan ISP. Perangkat yang digunakan adalah ZTE ZXHN F670L, dengan spesifikasi mendukung jaringan nirkabel 5G dan 2.4G (802.11b/g/n), dilengkapi 4 port Gigabit Ethernet, 1 port telepon, USB 2.0, WiFi (2x2), port SC/APC, kecepatan downstream 2,448 Gbit/s dan upstream 1,244 Gbit/s.

Router Mikrotik yang digunakan adalah Mikrotik RouterBoard RB750gr3 (hEX), sebuah perangkat yang memungkinkan pengoperasian jaringan tanpa memerlukan instalasi sistem operasi pada komputer. Perangkat ini memiliki CPU berkecepatan 880 MHz dengan 2 inti dan 4 thread, RAM 256 MB, penyimpanan 16 MB, 5 port Gigabit, serta lisensi RouterOS Level 4.

Sementara itu, perangkat Optical Line Termination (OLT) berfungsi sebagai titik akhir jaringan optik pasif (PON), yang menghubungkan jaringan pusat dengan perangkat pelanggan, serta mengatur komunikasi di antara keduanya. Jenis OLT yang digunakan adalah HSGQ-E04R, dengan fitur-fitur seperti Wireless LAN, kabel LAN, protokol Onvif dan TCP/IP, POE, serta 4 port EPON dengan jangkauan transmisi hingga 20 km.

Pada tahap wawancara, diperoleh beberapa hal yang diperlukan terkait penelitian.Permasalahan yang muncul berkaitan dengan kerentanan sistem keamanan jaringan di Sahabat Net. Saat ini, hak akses jaringan masih dapat diakses oleh pihak lain, terutama ketika perangkat jaringan di ruang server diakses melalui jaringan lokal. Kondisi ini menimbulkan potensi terjadinya peretasan atau penyadapan, karena proses komunikasi berlangsung melalui jaringan publik saat mengakses sumber daya yang seharusnya bersifat privat.

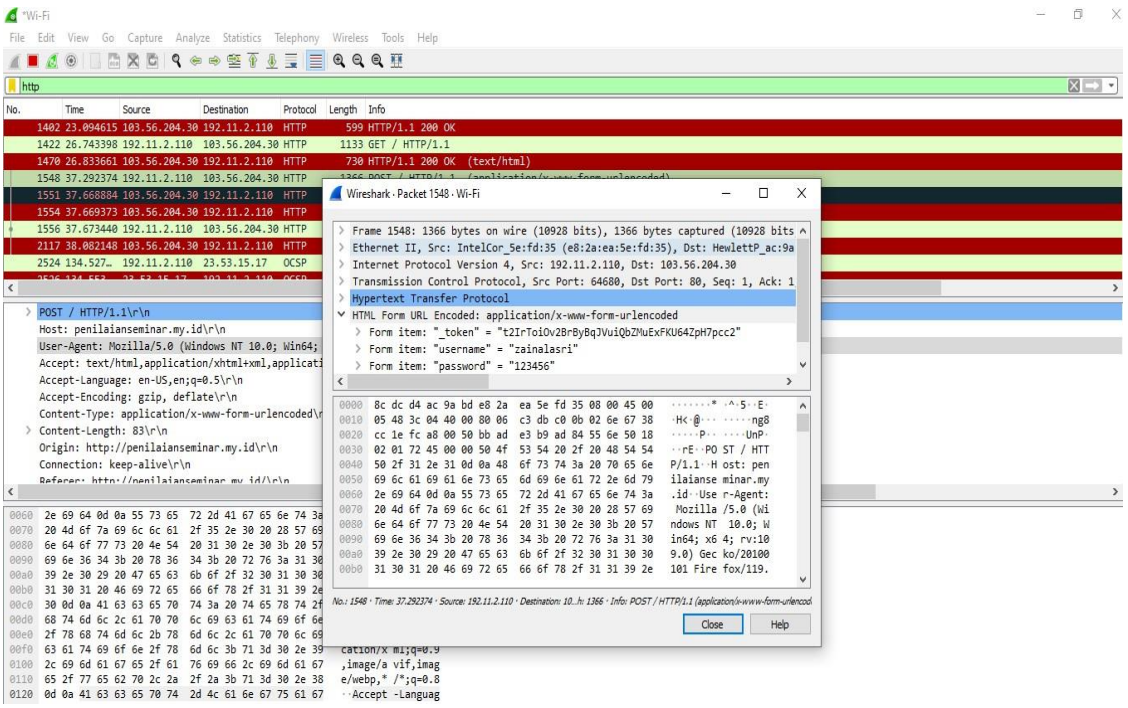
Pengumpulan data dan informasi dilakukan untuk mengidentifikasi permasalahan yang terjadi pada jaringan Sahabat Net. Dalam jaringan ini, terdapat sebanyak 183 klien yang terhubung, serta menggunakan jaringan nirkabel (WiFi) dengan kapasitas bandwidth sebesar 300 Mbps. Untuk keperluan pengujian, peneliti menggunakan dua unit laptop: satu berfungsi sebagai perangkat penyerang, dan satu lagi sebagai target. Proses pengambilan data dilakukan dengan bantuan aplikasi Wireshark, yang digunakan untuk melakukan sniffing guna memperoleh informasi seperti username dan password yang ditransmisikan melalui jaringan Sahabat Net. Gambar 2 di bawah ini menunjukkan topologi jaringan yang digunakan di Sahabat Net.



Gambar 2. Topologi Jaringan Sahabat Net.

2.2. Pengukuran Jaringan Existing

Untuk mengetahui kondisi jaringan pada jaringan Sahabat Net sebelum di lakukan keamanan jaringan maka dilakukan penguji.dapat dilihat pada gambar 3.dibawah ini.

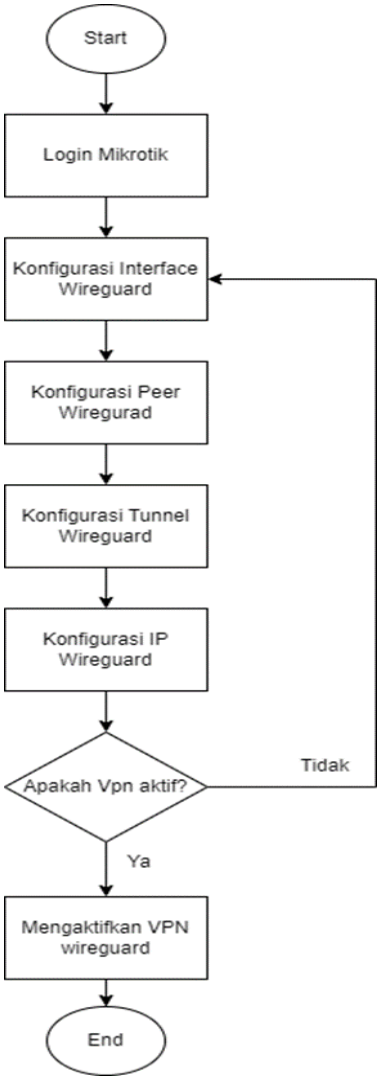


Gambar 3. Hasil Pengujian jaringan Existing.

Pengujian keamanan dilakukan dengan penyerangan *sniffing* menggunakan *software wireshark*. *sniffing* di arahkan dengan ip target 192.11.2.110 maka keluar hasil *username* (zainalasri) dan *password* (123456) Dari hasil pengujian tersebut terdapat sistem keamanan Jaringan pada Sahabat Net masih dapat disadap.

2.3. Penerapan VPN WireGuard

Pada tahap ini, konfigurasi dilakukan dengan memanfaatkan perangkat lunak WinBox, yang berfungsi untuk mengakses dan mengelola *server* Mikrotik melalui antarmuka grafis (GUI). Implementasi dilakukan pada *router* Mikrotik, dengan fokus utama pada konfigurasi *firewall* agar *server* VPN dapat diakses dan digunakan oleh pengguna dari publik. Pada gambar 4 merupakan tahapan untuk penerapan VPN WireGuard.



Gambar 4. Flowchart Konfigurasi *Wireguard*

Pada tahap konfigurasi WireGuard, langkah awal yang dilakukan adalah mengakses perangkat Mikrotik dan membuat interface VPN WireGuard agar dapat tersambung ke internet. Proses ini dimulai dengan membuka menu WireGuard, lalu klik "Add", pilih tab "General", beri nama interface (misalnya "wireguard1"), kemudian klik "Apply" dan "OK". Setelah itu, sistem akan otomatis menghasilkan private key, public key, dan nilai MTU. Public key ini nantinya digunakan untuk menambahkan peer pada perangkat klien. Selanjutnya, diberikan alamat IP pada interface WireGuard tersebut.

Untuk menambahkan peer agar koneksi VPN dapat terbentuk, buka kembali menu WireGuard, pilih bagian "Peer", klik "Add", lalu pilih interface "wireguard1", masukkan public key yang diperoleh dari aplikasi WireGuard di sisi klien, dan tentukan alamat pada kolom "Allowed Addresses".

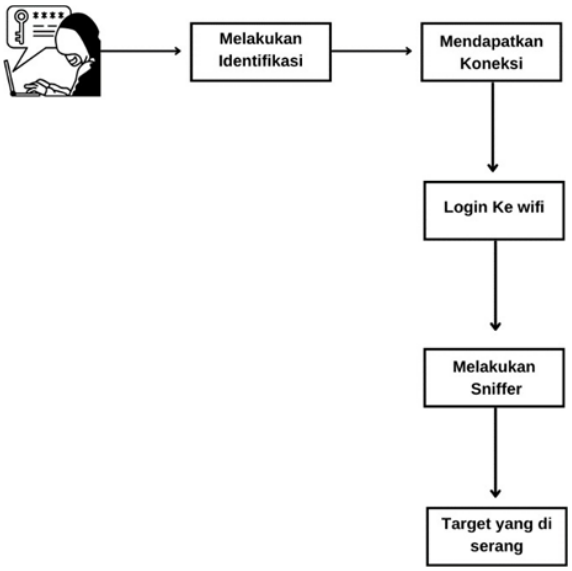
Setelah konfigurasi peer di Mikrotik selesai, lanjutkan dengan pengaturan di aplikasi WireGuard pada perangkat klien. Klik ikon segitiga di samping "Add Tunnel", pilih "Add Empty Tunnel", beri nama (misalnya "tes"), dan sesuaikan alamat "Allowed Address" dengan yang telah diatur di peer Mikrotik. Masukkan DNS 8.8.8.8, lalu pada bagian peer, salin *public key* dari interface WireGuard di Mikrotik. Isikan "Allowed IPs" dengan 0.0.0.0/0, dan masukkan IP publik serta port dari interface WireGuard Mikrotik pada kolom "Endpoint".

Langkah terakhir adalah menambahkan IP pada interface WireGuard di Mikrotik agar VPN bisa terkoneksi. Buka menu "IP", lalu pilih "Address", klik "Add", masukkan alamat IP 192.168.50.1/24, pilih interface "wireguard1", kemudian klik "Apply" dan "OK". Setelah seluruh tahapan selesai, koneksi VPN menggunakan WireGuard telah berhasil dikonfigurasi dan siap digunakan.

2.4. Skenario Pengujian Keamanan Jaringan.

Tahap ini bertujuan untuk menguji apakah sistem yang telah dikembangkan dapat berfungsi dengan baik dan sesuai dengan tujuan dari penelitian, yaitu untuk mengevaluasi peningkatan kualitas keamanan jaringan. Proses pengujian dilakukan dengan melakukan *sniffing* menggunakan perangkat lunak Ettercap.

Pengujian keamanan informasi dilakukan untuk mengidentifikasi celah keamanan informasi pada jaringan kabel dan *Wireless* (*Wireless* LAN). Pengujian keamanan jaringan dilakukan dengan menggunakan serangan *Sniffing*. *Sniffing* adalah teknik serangan yang melakukan pemantauan atau mengontrol setiap paket yang dikirim melalui media komunikasi kabel atau nirkabel [16]. Ini dilakukan melalui perangkat lunak atau perangkat keras yang memantau lalu lintas yang masuk ke jaringan. Perangkat lunak *Ettercap* dan *Wireshark* digunakan untuk melakukan serangan *sniffing*. Skenario Pengujian *sniffing* dapat dilihat pada gambar 5.



Gambar 5. Skenario Pengujian *Sniffing*

Pengujian dilakukan dengan membandingkan kondisi jaringan sebelum dan sesudah penerapan WireGuard, untuk menilai tingkat keamanan yang dihasilkan. Analisis lalu lintas jaringan dilakukan menggunakan aplikasi Wireshark pada jaringan Sahabat Net, dengan tahapan sebagai berikut:

a) Pada tahap awal, koneksi ke jaringan diperoleh oleh peneliti, dan jaringan dimasuki sebagai pengguna.
b) Aktivitas pengguna yang terhubung ke jaringan Sahabat Net direkam (di-*capture*) untuk dianalisis.
c) Salah satu pengguna yang terhubung ke jaringan diminta melakukan proses login guna diperoleh alamat IP target.

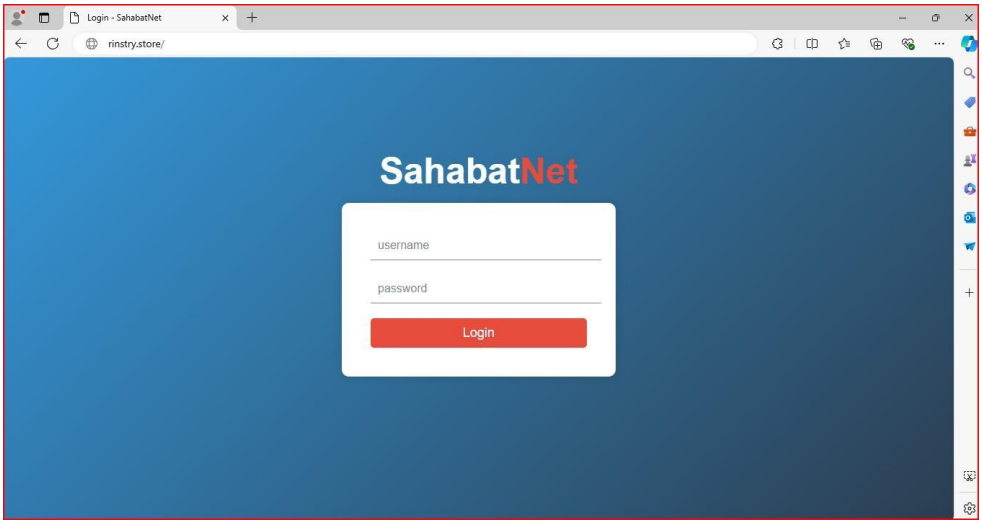
Untuk pengujian serangan *sniffing* menggunakan perangkat lunak Ettercap, langkah-langkah berikut diterapkan:

a) Keamanan jaringan yang akan diserang diidentifikasi terlebih dahulu.
b) Setelah proses identifikasi dilakukan, jaringan dimasuki oleh peneliti sebagai pengguna.
c) Alamat IP yang terhubung ke jaringan Sahabat Net dipindai (di-scan).
d) IP *address* target ditentukan untuk dilakukan penyadapan paket data.
e) Serangan ARP poisoning dilakukan terhadap IP yang telah ditentukan.ktivitas jaringan dari IP target
f) kemudian dianalisis untuk memantau lalu lintas data yang terjadi.

3. HASIL DAN PEMBAHASAN

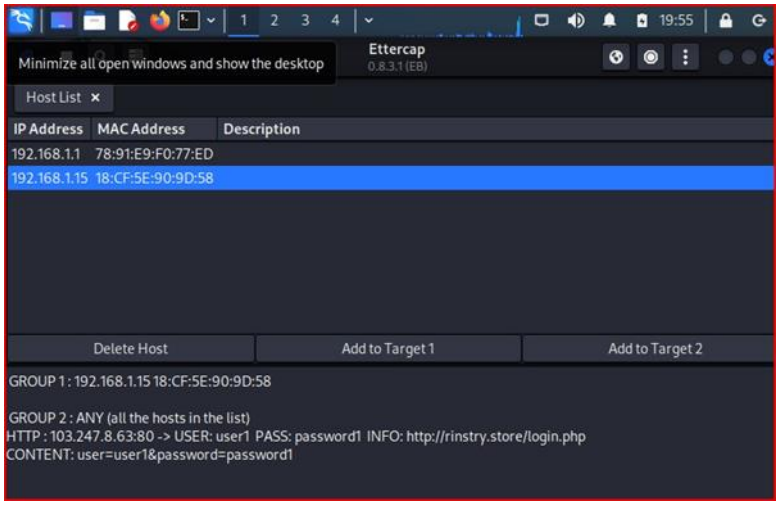
3.1 Hasil Pengujian *Sniffing Ettercap* Sebelum Menggunakan VPN Wireguard.

Sebelum melakukan pengujian menggunakan ettercap memerlukan halaman login untuk di uji. Gambar 7 dibawah adalah halaman login web yang akan di uji. Pada gambar 7 saat melakukan penyerangan terdapat salah satu akun yang login ketika sedang mengaksesnya menggunakan wifi yang berada di SahabatNet.



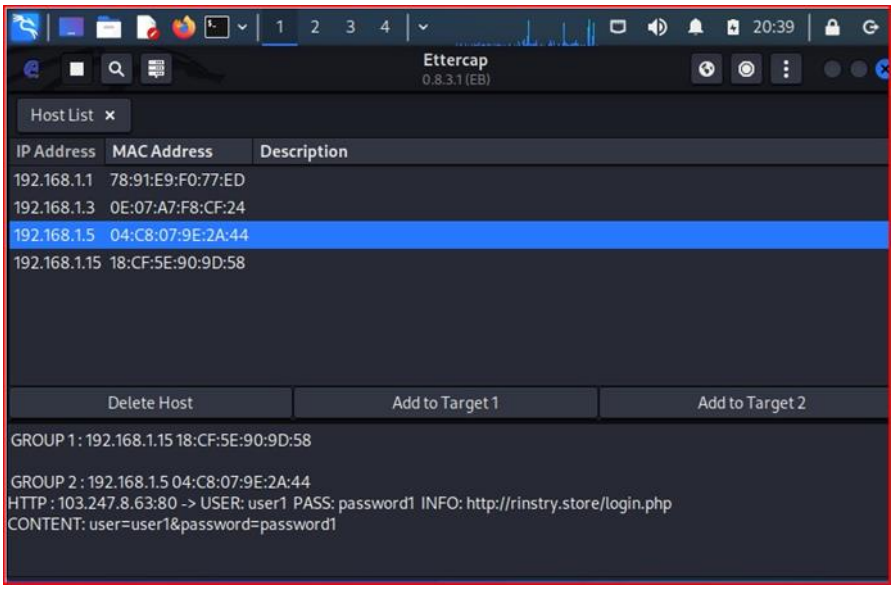
Gambar 7. Halaman Login pada SahabatNet

Berikut merupakan hasil pengujian sebelum menerapkan *Wireguard*, dapat dilihat pada Gambar 8 dan Gambar 9.



Gambar 8 Hasil penyerangan menggunakan Ettercap pada Target 1.

Gambar 8 menunjukkan hasil serangan yang dilakukan menggunakan aplikasi Ettercap. Dalam gambar tersebut, terdeteksi dua host dalam jaringan, yaitu 192.168.1.1 dan 192.168.1.15. Host dengan alamat IP 192.168.1.15 dijadikan sebagai target serangan (Group 1), sementara Group 2 merepresentasikan seluruh host yang ada dalam daftar jaringan. Melalui serangan ini, kredensial login berhasil ditangkap oleh Ettercap, yakni username: **user1** dan password: **password1**, yang diperoleh dari koneksi HTTP menuju URL **http://rinstry.store/login.php**. Serangan ini dimungkinkan karena lalu lintas data masih menggunakan protokol yang tidak terenkripsi (HTTP), sehingga informasi sensitif dapat diambil melalui teknik **ARP spoofing**.



Gambar 9. Hasil penyerangan menggunakan Ettercap pada Target 2.

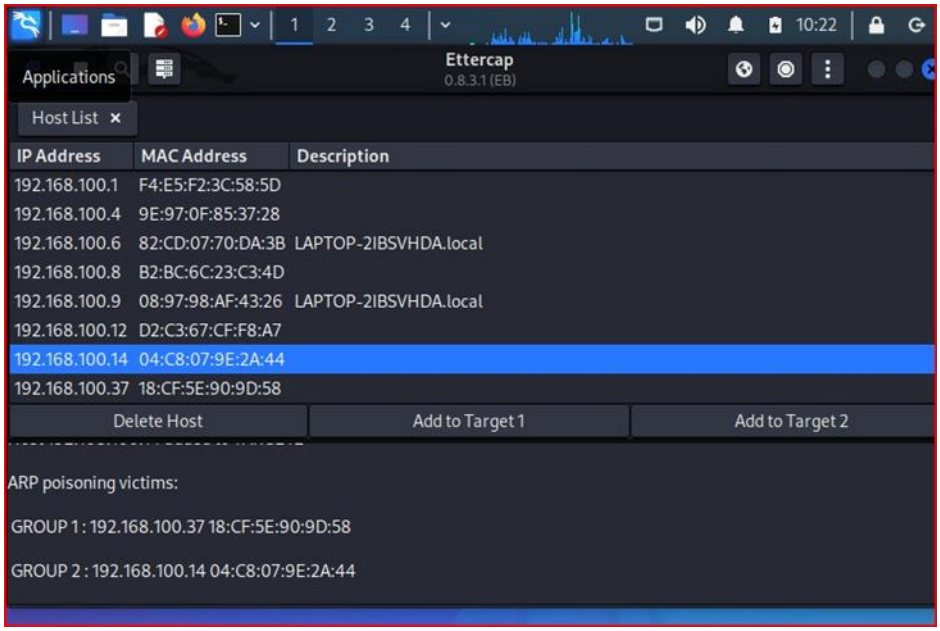
Gambar 9 menampilkan hasil serangan yang dilakukan menggunakan aplikasi Ettercap pada jaringan lokal. Dalam proses ini, terdeteksi empat host, yaitu 192.168.1.1, 192.168.1.3, 192.168.1.5, dan 192.168.1.15. Host dengan alamat IP 192.168.1.15 ditetapkan sebagai target utama (Group 1), sementara 192.168.1.5 dijadikan sebagai target tambahan (Group 2). Melalui serangan ini, informasi sensitif berhasil disadap dari koneksi HTTP yang tidak dilindungi enkripsi, termasuk kredensial login berupa username: user1 dan password: password1, yang dikirim ke alamat URL http://rinstry.store/login.php. Serangan ini diperkirakan dilakukan dengan metode *ARP spoofing*, yang memungkinkan pengalihan lalu lintas jaringan melalui perangkat penyerang. Gambar tersebut memperlihatkan hasil proses *sniffing* terhadap target. Data hasil *sniffing* dapat dilihat pada table 1.

Tabel 1. Data hasil *sniffing* sebelum Menggunakan VPN.

	Target 1	**Target 2**
Alamat IP	192.168.15	192.168.1.5
Alamat Mac	18:CF:5E:90:9D:58	04:C8:07:9E:2A:44
Username	User1	User1
Password	*Password*1	*Password*1

3.2 Hasil Pengujian *Sniffing Ettercap* Setelah Mengunakan VPN WireGuard.

Pada Gambar 10 di bawah merupakan hasil penyerangan packet *sniffing* setelah melakukan Analisis Sistem Keamanan Menggunakan *Wireguard*



Gambar 10. Hasil penyerangan setelah penerapan *Wireguard*

Pada Gambar 10, diperlihatkan situasi di mana serangan sniffing dilakukan untuk memantau lalu lintas jaringan, namun log aktivitas dari perangkat target tidak dapat ditampilkan. Perangkat dengan alamat IP 192.168.100.37 telah diidentifikasi sebagai router Mikrotik yang digunakan sebagai klien WireGuard VPN. Selain itu, perangkat lain dengan alamat IP 192.168.100.14, yang merupakan sistem operasi Windows, juga telah digunakan sebagai klien WireGuard VPN. Kedua perangkat tersebut telah dikonfigurasikan untuk berkomunikasi melalui jaringan yang diamankan oleh protokol WireGuard.

Dalam pengujian, akses terhadap halaman login tertentu telah dilakukan oleh peneliti guna memicu lalu lintas jaringan yang dapat disadap. Namun, hasil penyadapan tidak menunjukkan adanya log aktivitas yang dapat dianalisis. Hal ini menunjukkan bahwa komunikasi yang berlangsung telah berhasil dienkripsi dengan baik oleh protokol WireGuard, sehingga tidak dapat dibaca atau diinterpretasikan oleh pihak ketiga.

Enkripsi menyeluruh yang diterapkan oleh WireGuard telah digunakan untuk mengamankan lalu lintas antara klien dan server, sehingga seluruh data yang dikirimkan melalui jaringan tidak dapat diakses oleh penyerang, termasuk yang menggunakan teknik sniffing. Berdasarkan hasil pengamatan, dapat disimpulkan bahwa teknik sniffing tidak mampu digunakan untuk menyadap komunikasi yang telah diamankan oleh protokol WireGuard, sehingga efektivitas protokol ini dalam menjaga kerahasiaan dan integritas data dapat dikonfirmasi. Berikut pada table 2 merupakan hasil penyadapan *sniffing* setelah melakukan analisis sistem keamanan menggunakan *wireguard.*

Tabel 2. Data hasil *sniffing* sebelum Menggunakan VPN.

	Target 1	**Target 2**
Alamat IP	192.168.100.37	**192.168.100.14**
Alamat Mac	18:CF:5E:90:9D:58	**04:C8:07:9E:2A:44**
Username	-	-
Password	-	-

3.3 Pembahasan

Sebelum penggunaan VPN *WireGuard*, dilakukan simulasi pengujian keamanan jaringan lokal dengan memanfaatkan tools Ettercap untuk mengevaluasi sejauh mana kerentanan data terhadap serangan *sniffing*. Metode yang digunakan adalah ARP *spoofing*, yakni manipulasi *cache ARP* agar data yang dikirimkan oleh host korban dialihkan ke perangkat penyerang. Hasil dari serangan ini tampak pada Gambar 8, di mana lalu lintas jaringan berhasil dicegat dan ditampilkan secara *real-time*. Alamat IP target (192.168.1.15) terdeteksi mengakses situs login yang menggunakan protokol HTTP tanpa enkripsi, sehingga informasi penting seperti nama pengguna dan kata sandi dapat terbaca dengan jelas.

Analisis yang lebih luas dilakukan pada Gambar 9, di mana Ettercap mendeteksi empat perangkat aktif dalam jaringan. Penyerang kemudian menetapkan dua target utama, yakni IP 192.168.1.15 sebagai Group 1 dan IP 192.168.1.5 sebagai Group 2. Setelah proses ARP spoofing dilakukan, data login yang dikirimkan oleh kedua target berhasil disadap, dengan isi yang sama yaitu username "user1" dan password "password1", yang dikirim ke alamat http://rinstry.store/login.php. Keberhasilan Ettercap dalam menangkap data dari dua target sekaligus menunjukkan bahwa jaringan tersebut sangat rentan, terutama karena protokol HTTP memungkinkan transmisi data tanpa perlindungan enkripsi.

Berdasarkan hasil pengamatan dari table 1 yang disusun, dapat disimpulkan bahwa jaringan dalam kondisi ini tidak memiliki perlindungan yang memadai terhadap intersepsi data. Ketika protokol komunikasi tidak dienkripsi dan tidak ada perlindungan tambahan seperti VPN, kredensial pengguna dapat dengan mudah dicuri oleh pihak tidak bertanggung jawab. Oleh karena itu, penting untuk menerapkan mekanisme keamanan seperti VPN *WireGuard*, yang mampu mengenkripsi seluruh data lalu lintas jaringan. Dengan demikian, meskipun data berhasil ditangkap oleh penyerang, isi komunikasi tetap terlindungi dan tidak dapat diinterpretasikan secara langsung.

Setelah implementasi protokol WireGuard pada jaringan Sahabat Net, dilakukan pengujian untuk mengevaluasi sejauh mana keamanan lalu lintas data dapat ditingkatkan. Pengujian dilakukan dengan metode sniffing menggunakan aplikasi Ettercap, di mana dua perangkat ditargetkan: satu menggunakan alamat IP 192.168.100.37 (router Mikrotik) dan yang lain menggunakan IP 192.168.100.14 (perangkat Windows). Keduanya telah dikonfigurasi sebagai klien WireGuard. Hasil pemindaian menunjukkan bahwa perangkat berhasil dikenali dan ditetapkan sebagai target ARP poisoning, namun tidak ada lalu lintas data sensitif yang dapat ditampilkan dalam bentuk log atau isi komunikasi.

Ketika penyerang mencoba memantau komunikasi antara kedua klien VPN tersebut, tidak ditemukan informasi seperti username maupun password yang sebelumnya dapat diperoleh saat jaringan belum menggunakan protokol *WireGuard*. Hal ini membuktikan bahwa enkripsi end-to-end yang diterapkan oleh WireGuard bekerja secara efektif. Meskipun aktivitas pengguna telah dipicu dengan membuka halaman login untuk menghasilkan lalu lintas jaringan, seluruh isi paket yang ditransmisikan tetap tersembunyi dari upaya sniffing, sehingga tidak dapat dibaca ataupun dianalisis oleh pihak ketiga.

Dari hasil ini dapat disimpulkan bahwa penggunaan *WireGuard* mampu menghilangkan celah terhadap serangan sniffing, bahkan saat metode *ARP poisoning* digunakan untuk menyusup ke dalam lalu lintas jaringan. Kriptografi modern yang diadopsi WireGuard, seperti Curve25519 untuk enkripsi kunci publik, memberikan proteksi kuat yang tidak memungkinkan dekripsi data secara pasif. Ini membuktikan bahwa penerapan *WireGuard* bukan hanya sekadar menambah lapisan keamanan, namun juga efektif dalam menjaga kerahasiaan, integritas, dan privasi komunikasi digital antarperangkat dalam jaringan lokal.

4. KESIMPULAN

Berdasarkan latar belakang permasalahan dan tujuan yang telah dirumuskan, dapat disimpulkan bahwa kondisi jaringan pada Sahabat Net sebelum diimplementasikannya protokol VPN WireGuard masih rentan terhadap serangan sniffing. Hasil pengujian menunjukkan bahwa melalui metode sniffing, informasi sensitif seperti username dan password yang digunakan dalam proses autentikasi dapat

diperoleh secara tidak sah. Namun, setelah penerapan protokol WireGuard VPN, tingkat keamanan jaringan meningkat secara signifikan. Hal ini dibuktikan melalui pengujian lanjutan, di mana tidak ditemukan log aktivitas berupa data kredensial selama proses sniffing berlangsung. Dengan demikian, penerapan WireGuard VPN terbukti efektif dalam mencegah penyadapan data dan melindungi komunikasi jaringan dari potensi ancaman eksternal.

Daftar Pustaka

[1] S. Bumbungan, "Peran Dan Perkembangan Jaringan Internet Dalam Mendukung Transformasi Digital Global," *Bulletin Of Network Engineer And Informatics*, Vol. 3, No. 1, P. 11, Apr. 2025, Doi: 10.59688/Bufnets.V3i1.66.

[2] S. Scherrer, S. Tabaeiaghdaei, And A. Perrig, "Quality Competition Among Internet Service Providers," Aug. 2023, [Online]. Available: Http://Arxiv.Org/Abs/2305.06811

[3] M. Jufri, "Peningkatan Keamanan Jaringan Wireless Dengan Menerapkan Security Policy Pada Firewall," *Joisie Journal Of Information System And Informatics Engineering*, Vol. 5, No. Desember, Pp. 98–108, 2021.

[4] A. Imran And A. Rustianto, "Analisis Dan Implementasi Interkoneksi Jaringan Komputer Berbasis Vpnl2tp Ipsec Pada Smk Tkj Di Depok ," *Jurnal Informatika Terpadu* , Vol. 7, No. 1, Pp. 33–38, Mar. 2021.

[5] H. Jumakhan And A. Mirzaeinia, "Wireguard: An Efficient Solution For Securing Iot Device Connectivity," Feb. 2024, [Online]. Available: Http://Arxiv.Org/Abs/2402.02093

[6] Zuhe Liu, "Application And Security Analysis Of Virtual Private Network (Vpn) In Network Communication," *Academic Journal Of Computing & Information Science*, Vol. 6, No. 11, 2023, Doi: 10.25236/Ajcis.2023.061108.

[7] I. K. Rahman And L. N. Harnaningrum, "Analisa Quality Of Service (Qos) Pada Jaringan L2tp Ipsec Dan Wireguard Vpn Untuk Mengamankan Voip," *Jurnal Resistor*, Vol. 3, No. 1, Pp. 10–20, 2020, [Online]. Available: Https://S.Id/Jurnalresistor

[8] Bongga Arifwidodo, "Mekanisme Keamanan Jaringan Menggunakan Protokol Wireguard Pada Jaringan Privat," *Journal Of Informatics And Communication Technology* , Vol. 5, No. 2, Pp. 78–86, Dec. 2023, Doi: Https://Doi.Org/10.52661/J_Ict.V5i2.211.

[9] R. Hermawan And Y. M. Saputra, "Analisis Perbandingan Penggunaan Metode Tunneling Cloud Virtual Private Network Dan Wireguard Virtual Private Network Pada Implementasi Infrastruktur Hybrid Cloud," *Journal Of Internet And Software Engineering*, Vol. 6, No. 1, 2025.

[10] T. S. Ali, I. Santoso, A. S. Quiko, G. Santoso, U. Teknologi, And M. Jakarta, "Jarekom: Jurnal Jaringan Dan Rekayasa Komputer Pengaruh Virtual Private Network (Vpn) Terhadap Keamanan Dan Performa Akses Jaringan," Jun. 2025, Doi: 10.9020/Jarekom.V1i1.

[11] L. O. Sari And H. Helena, "Implementasi Virtual Private Network Menggunakanlayer 2 Tunneling Protocol Berbasis Mikrotik," *Malcom: Indonesian Journal Of Machine Learning And Computer Science*, Vol. 4, No. 4, Pp. 1496–1504, Sep. 2024, Doi: 10.57152/Malcom.V4i4.1651.

[12] R. Elsya Putra *Et Al.*, "Mengamankan Serangan Packet Sniffing Pada Jaringan Komputer Menggunakan Vpn Tunnel," *Jurnal Sains Manajemen Informatika Dan Komputer*, Vol. 22, No. 2, Pp. 340–347, 2023, Doi: Https://Doi.Org/10.53513/Jis.V22i2.7438.

[13] Ade Frihadi, "Perancangan Interkoneksi Jaringan Menggunakan Vpn Berbasis Internet Dengan Implementasi Ipv6," *Jurnal Ekselenta*, Vol. 1, No. 1, 2024.

[14] D. Novianto, Y. S. Japriadi, And L. Tommy, "Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard Vpn Di Routerboard Mikrotik," *Jurnal Ilmiah Informatika Global*, Vol. 13, No. 2, Aug. 2022, Doi: 10.36982/Jiig.V13i2.2308.

[15] J. Literasiologi Literasi Kita Indonesia, T. Wulandari, D. Purnama Sari, And A. Rahmi Nasution, "Deskripsi Mendalam Untuk Memastikan Keteralihan Temuan Penelitian Kualitatif," *Jurnal Literasiologi*, Vol. 11, No. 2, 2023, Doi: 10.47783/Literasiologi.V9i4.

[16] Tamsir Ariyadi, "Analisis Keamanan Jaringan Wifi Mahasiswa Ubd Dari Serangan Packet Sniffing," *Jurnal Ilmiah Informatika*, Vol. 12, No. 1, 2024, Doi: Https://Doi.Org/10.33884/Jif.V12i01.8739.