CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 6, No. 2, November 2023, hlm. 30-38

Keamanan Jaringan *Wi-Fi* Terhadap Serangan *Packet Sniffing* Menggunakan *Firewall Rule* (Studi Kasus : Pt. Akurat.Co)

Arini[1] , Muhammad Luthfi Arsalan[2], Husni Teja Sukmana[3]

[1,2,3]Teknik Informatika, Fakultas Sain dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah Jakarta
Email: [1]arini@uinjkt.ac.id, [2]luthfiarsalan34@gmail.com, [3]husniteja@uinjkt.ac.id

Abstrak

Wifi sangat rentan terhadap berbagai ancaman serangan seperti *packet sniffing*, sistem keamanan dan identifikasi yang baik diperlukan untuk mencegah serangan oleh oknum yang tidak bertanggung jawab. PT Akurat.co merupakan perusahaan media berita yang bergerak dibidang teknologi informasi yang berpotensi terjadi permasalahan keamanan jaringan karena terdapat *port-port* terbuka dan pengimplementasian topologi jaringan yang tidak aman. Untuk mengatasi masalah tersebut terdapat beberapa cara, berupa pencegahan dan pendeteksian. Salah satu bentuk pencegahan adalah *firewall rule* fitur yang terdapat di *Mikrotik Router* OS berfungsi sebagai pemberi akses paket koneksi. Metode simulasi menjadi dasar pada penelitian ini untuk mensimulasikan kejadian serangan pada *wifi*. Dengan adanya proses pengujian untuk sistem keamanan jaringan *wifi* yang berupa usaha penyusupan dengan percoban serangan *arp spoofing* untuk mencari *username* dan *password* dan percobaan *scanning port* untuk mencari *port* yang terbuka dan percobaan serangan *ddos attack* untuk mengirimkan paket ke target dan mengimplementasikan *firewall rule* terhadap serangan yang telah dilakukan. *Firewall rule* berhasil melakukan *action drop* terhadap seranga *arp spoofing* sehingga serangan tersebut dapat diproteksi, *action tartip* berhasil mengecoh *port* yang tebuka adalah *port* tipuan dan berhasil melakukan *drop* terhadap pengiriman paket yang banyak. Sehingga sistem keamanan jaringan terjaga dengan aman, dan setiap aktivitas peretasan berhasil di cegah oleh *firewall rule* mikrotik.

Kata kunci: *keamanan jaringan, wireless fidelity, packet sniffing, firewall rule mikrotik router os.*

Wi-Fi Network Security Against Packet Sniffing Attacks Using Firewall Rule (Case Study : Pt. Accurate.Co)

Abstract

Wifi is very vulnerable to various threats, such as packet sniffing. Good security and identification systems are needed to prevent attacks by irresponsible people. PT Akurat.co is a news media company operating in the field of information technology that has potential network security problems due to the existence of open ports and the implementation of an unsafe network topology. There are several ways to deal with the problem: prevention and detection. One form of precaution is the firewall rule feature that is present in Mikrotik Router OS and serves as the access provider for the connection package. The simulation method forms the basis for this research to simulate attacks on WiFi. With the testing process for the wifi network security system, there is an intrusion attempt with an arp spoofing attack attempt to find a username and password, a port scanning experiment to find an open port, and an attempt at a DDoS attack to send a package to the target. Implement a firewall rule against an attack that has been carried out. The firewall rule successfully performed an action drop against an arp spoofing attack so that the attack can be protected. The action tartip successfully blocked the port that was opened as a fraudulent port and successfully executed an action drop against the delivery of many packages. So the network security system is awake safely, and any hacking activity is successfully prevented by a Mikrotik firewall rule.

Keywords*: Network security, wireless fidelity, packet sniffing, firewall rule mikrotik router os.*

1. PENDAHULUAN

Pada saat ini, kemajuan dan perkembangan teknologi telah berkembang sangat pesat khususnya dibidang informasi dimana masyarakat memanfaatkan teknologi ini untuk kegiatan seperti mencari informasi, berbagi data dengan teman, bertransaksi keuangan melalui fasilitas *e-bangking*, serta berinteraksi social menggunakan layanan aplikasi social media da lain-lain(Hae, 2021).

WiFi singkatan dari kesetiaan *nirkabel*. *Wi-Fi* adalah teknologi untuk bertukar data dengan menggunakan gelombang radio (*nirkabel*) yang dapat digunakan di berbagai perangkat elektronik seperti komputer, smartphone, tablet dan lainnya(Gunawan, 2021).

Berdasarkan Observasi penulis pada tanggal 1 Februari 2023 di PT Akurat Sentra Media adalah perusahaan media berita digital, entertaiment & advertising yang bergerak dalam bidang teknologi

khususnya penyedia jasa media berita online melalui website dan sosial media. Tedapat satu server dan jaringan internet yang terpasang dalam lingkup kantor media tersebut, yaitu data base server dan jaringan internet *wifi* atau local area network (LAN) untuk memenuhi kebutuhan di kantor tersebut seperti website media berita, pengelolaan sosial media, *event organizer* dan jasa survey online.

Keamanan jaringan menurut Gustiawan, adalah sistem yang dipakai agar terhindar dari ancaman luar yang dapat merusak jaringan serta ancaraman dari dalam, seperti ancaman pencurian data perusahaan, jebolnya sitem karena password yang diketahui oleh orang yang tidak berhak dan segala macam seranga dan usaha-usaha penyusupan atau pemindaian dengan cara memberikan proteksi atau perlindungan pada jaringan *wifi*(Gustiawan et al., 2021). Sedangkan keberadaan perangkat jaringan router wireless saat ini memiliki banyak celah keamanan dan dapat diekploitasi oleh pihak yang tidak bertanggung jawab, seperti pada router wireless rumahan xiaomi(Hariyadi et al., 2021).

Saat ini dalam sistem keamanan jaringan di PT Akurat Sentra Media belum terdapat sistem keamanan jaringan pada perusahaan tersebut dan semakin banyak jumlah komputer (user) yang tehubung dengan jaringan internet lokal maupun publik pada PT Akurat Sentra Media maka probabilitas ancaman dan serangan *packet sniffing* pada sistem keamanan jaringan tentu tidak dapat dihindari. Proteksi keamanan jaringan *wifi* sangatlah penting untuk mejaga keberlangsungan jaringan komputer perusahaan. Terutama untuk menjaga jaringan *wifi* dari segala macam akses ilegal yang mencoba untuk masuk dan mengelola jaringan yang ada perusahaan.

Packet sniffing adalah teknik untuk memantau setiap paket yang melewati suatu jaringan. *Sniffing paket* adalah perangkat lunak atau perangkat keras yang digunakan oleh penyadap untuk mengungkapkan semua lalu lintas masuk dan keluar, termasuk nama pengguna dan kata sandi, atau bahkan mengungkapkan port terbuka (Dharma and Thamrin, 2020).

Pada penelitian(Rizkiyani, 2020), yang berjudul analisi keamanan fasilitas *(wifi*) terhadap serangan *packet sniffing* penelitan ini menganalisis keamanan jaringan *wifi* terhadap serangan *packet sniffing* menggunakan tools inssider untuk mengidentifikasi *wifi* dan tools ettercap untuk menyerang jaringan *wifi* penelitian menggunakan metode intrusion detection sistem (IDS) dan penelitian ini mendapatkan *wifi* kantor koran seruya terdapat pada *access point* yang terdapat pada *wifi* hanya menyediakan satu buah accses point tidak terlalu efesien.

Pada penelitian yang berjudul analisis dan impelentasi keamanan jaringan pada *mikrotik router os* menggunakan metode *port knocking* dimana peneliti mengimplementasikan metode port knocking untuk meningkatkan keamanan jaringan dari penetrasi yang dilakukan oleh para hacker untuk menjaga hak akses diterapkan pada mikrotik router os dengan cara kerja yaitu dapat membuka atau menutup akses port tertentu melalui *firewall* pada router sesuai dengan role yang dibangun (Amarudin, 2018).

Setelah melakukan analisis terhadap permasalahan di atas dengan berlandaskan beberapa literatur, hal tersebut melatar belakangi penulis untuk melakukan penelitian dengan topik "Keamanan Jaringan *Wireless Fidelity* (*Wi-Fi*) Terhadap Serangan *Packet Sniffing* Menggunakan *Firewall Rule* (Studi Kasus: PT Akurat Sentra Media).

2. TINJAUAN PUSTAKA

2.1. Jaringan *Wi-Fi*

Jaringan *WiFi* berarti presisi *nirkabel*. *Wi-Fi* adalah teknologi untuk bertukar data melalui gelombang radio (*nirkabel*) yang dapat digunakan di berbagai perangkat elektronik seperti komputer, *smartphone*, tablet, dan sebagainya (Junita et al., 2013).

2.2. Monitoring Jaringan

Monitoring jaringan yaitu suatu proses rutin pengambilan data dan kinerja kemajuan dari networking yang akan selalu memantau pada setiap perubahan yang akan terjadi pada jaringan tersebut untuk mempertahankan manajememen jaringan yang ada dan untuk memberitahukan berfungsi atau tidaknya suatu perangkat tersebut yang terhubung kedalam jaringan itu (Dharma and Thamrin, 2020).

2.3. Keamanan Jaringan

Keamanan jaringan merupakan sistem yang bekerja untuk pencegahan aktifitas yang tidak diinginkan dengan melakukan identifikasi pengguna yang tidak memiliki hak akses dalam suatu jaringan. Menghubungkan komputer dengan komputer lain baik menggunakan jaringan kabel atau nirkabel memungkinkan orang lain untuk mengakses data, mengubah isi, sampai menghapus data dalam jaringan tersebut (Al Fikri and Djuniadi, 2021).

2.4. Konsep Keamanan Jaringan

Tabel 1. Konsep Keamanan Jaringan

No.	Kategori	Penjelasan
1.	Resiko	Resiko berarti beberapa kemungkinan keberhasilan para penyusup dalam mengakses kedalam jaringan 19 sistem lokal yang dimiliki melalui konektivitas jaringan lokal ke Wide Area Network (WAN).
2.	*Denail of Service*	Menutup penggunaan utilitas jaringan normal dengan cara menghabiskan jatah central processing unit (CPU) memory maupun bandwidth.
3.	*Write Access*	Mampu melakukan proses menulis atau menghancurkan data dalam sistem.
4.	Ancaman	Pada dasarnya ancaman datang dari seseorang yang mempunyai keinginan memperoleh akses ilegal ke dalam suatu jaringan komputer.

No.	Kategori	Penjelasan
5.	Kerapuhan Sistem	Seberapa jauh menggambarkan perlindungan yang bisa diterapkan kepada network seseorang dari luar sistem yang berusaha memperoleh akses ilegal terhadap jaringan dan kemungkinan orang dari dalam sistem memberikan akses kepada dunia luar sehingga akan bersifat merusak sistem jaringan tersebut.
6.	*Access Control*	Membatasi dan mengontrol akses setiap pengguna.

2.5. OSI Layer

Lapisan OSI adalah model referensi untuk memahami jaringan komputer secara umum. Lapisan OSI juga dapat digunakan sebagai acuan untuk mengamankan jaringan (Ariyadi, 2018).

Jenis ancaman Keamanan jaringan *packet sniffing* termaksud dalam OSI layer diantaranya :

1. *Data Link Layer*

Lapisan tautan data bertanggung jawab untuk memeriksa kesalahan yang mungkin terjadi selama proses transmisi data dan juga untuk mengemas potongan-potongan tersebut ke dalam format bingkai data. Kerentanan pada lapisan ini dapat diserang oleh serangan yang menargetkan *address resolution protocol* (ARP) pada lapisan ini. Serangan ini memungkinkan peretas memanipulasi tabel *arp* jaringan untuk mengirimkan informasi ke alamat MAC yang salah.

2. *Network Layer*

Lapisan jaringan bertanggung jawab untuk menentukan jalur yang digunakan untuk mentransfer data antar perangkat di jaringan. Untuk mendukung proses perutean ini, lapisan jaringan menyimpan alamat, seperti alamat IP, untuk setiap perangkat di jaringan. Kerentanan pada lapisan ini dapat diserang oleh DDoS, yang dapat menonaktifkan jaringan DNS, yang dapat menyebabkan beberapa jaringan internet yang digunakan oleh situs web yang diakses pengguna menjadi mati (tidak bisa diakses).

3. *Transport Layer*

Lapisan transport bertanggung jawab untuk memindahkan orang antara dua atau lebih *host* di jaringan. Lapisan transport juga mengelola pemisahan dan penggabungan pesan dan juga memeriksa keandalan jalur komunikasi yang ditentukan. Protokol TCP adalah contoh lapisan transport yang paling umum digunakan.

2.6. Sniffing

Sniffing adalah suatu mekanisme, baik perangkat lunak maupun perangkat keras yang digunakan untuk memperoleh informasi yang melewati jaringan komputer menggunakan protokol apa saja. *Sniffing* itu sendiri memiliki beberapa macam diantaranya (Pranata, Abdillah and Ependi, 2015) :

1. *Arp Spoofing*

Arp Spoofing merupakan serangan inisiator dengan memanfaatkan kerentanan pada protokol ARP. Kerentanan ARP tidak akan melakaukan aurentikasi untuk memvalidasi arp-reply berasal dari perangkat yang benar. Secara singkat teknik serangan ini akan meracuni dan merusak tabel IP dengan menyisipkan MAC Address penyerang IP Address yang sah. Serangan ini menjadi inisiator serangan lanjutan, umumnya serangan dilancarkan berikutnya yaitu MITM.

2. *Port Scanning*

Port Scanning adalah tahapan awal untuk mendeteksi *port-port* yang terbuka dan mendapatkan informasi dari port yang terbuka pada target, servis apa yang sedang dijalankan, versi dari server dan lain sebgainya. Komunikasi dari Port scanning umumnya berada pada *layer transport protocol*, pada kasus tertentu *port scanning* akan terjadi pada session layer.

3. *Denail of Service*

Denail of Service (DOS) adalah salah satu jenis serangan dimana penyerangan menghabiskan sumber daya jaringan komputer. Dampak dari serangan DoS menyebabkan komputer tidak dapat berfungsi dengan normal.

2.7. InSSIDer, Ettercap, Nmap, LOIC, dan Wireshark

InSSIDer merupakan *software* untuk *scanner wifi* yang dapat bisa mengidentifikasi SSID, RRSI (kuat sinyal), *security* dan pengaturan yang ada pada accsess point (Riyanto, Rahmat and Zulfachmi, 2021).

Ettercap adalah merupakan *tools* salah satu cara untuk pengujian terhadap sistem keamanan jaringan *wifi* dimana *tools packet sniffer* ini dipergunakan untuk menganalisa protocol jaringan bebas dan digunakan untuk analisis *protocol* komputer jaringan dan mengaudit keamanan jaringan (Febriyanti Panjaitan, 2022).

Nmap (Network Mapper) adalah aplikasi atau alat yang melakukan pemindaian *port*. *Nmap* dibuat oleh Gordon Lyon, lebih dikenal sebagai Fyodor Vaskovich. Aplikasi ini digunakan untuk memeriksa jaringan yang ada (Jan William Tarigan, 2019).

LOIC adalah singkatan dari *low orbit ion cannon* atau bisa disebut LOIC Nonaktifkan server web. Ini adalah perangkat lunak DDOS yang paling kuat. Komunitas peretasan anonim telah terbukti menggunakan alat logika ini untuk aktivitas mereka. Perangkat lunak ini juga mematikan server facebook dari 60 server di seluruh dunia, meskipun hanya beberapa menit (Marta, Hartawan and Satwika, 2020).

Wireshark adalah *network protocol analyzer* adalah sebuah aplikasi perangkat lunak (*software*) yang digunakan untuk dapat melihat dan mencoba menangkap paket-paket jaringan dan berusaha untuk menampilkan semua informasi di paket tersebut sedetail mungkin. *Open source* dari *wireshark*

menggunakan *graphical user interface* (GUI) (Tri Novita et al., 2019).

2.8. Mikrotik dan Winbox

Mikrotik adalah sistem operasi dan perangkat lunak yang digunakan untuk memfungsikan komputer sebagai router. PC *router* tersebut dilengkapi dengan berbagai fasilitas dan alat, baik untuk jaringa kabel maupun *nirkabel*. *Mikrotik* sekarang ini banyak digunakan oleh ISP, penyedia hotspot, perusahaan-perusahaan *start-up*, ataupun oleh pemilik warnet (Suherdi, 2021).

Mikrotik Router OS memiliki fitur di dalamnya antara lain (I Dewa Made Bayu Atmaja Darmawan dan I Gede Oka Gatria Atitama, 2021) :

1. *Firewall*

Firewall ini adalah mekanisme yang diterapkan pada perangkat dan perangkat lunak yang dirancang untuk melindungi, membatasi, memfilter, dan bahkan menolak aktivitas atau segmen apa pun di jaringan lokal, meninggalkan jaringan eksternal di luar jangkauannya. *Firewall* bertanggung jawab untuk memastikan bahwa tidak ada penambahan yang dilakukan di luar batas yang diizinkan. Penggunaan teknologi informasi yang baik dan aman dalam membangun jaringan komputer sangatlah penting. Salah satu metode pengamanan jaringan yang dapat diterapkan adalah dengan menggunakan kemampuan dari *proxy server* yang dikenal dengan nama *proxy server*.

2. *Firewall Mangle*

Firewall mangle merupakan salah satu fitur firewall yang terdapat dalam mikrotik Router OS yang berfungsi sebagai penanda paket maupun koneksi data yang di request oleh user.

3. *Firewall Filter*

Firewall Filter adalah salah satu fungsi dari sistem operasi *router mikrotik* yang berperan sebagai barrier atau *provider* penggunaan paket koneksi. Di dalam aturan pemfilteran terdapat fungsi *drop* dan *accept* yang digunakan untuk memungkinkan akses paket koneksi, serta koneksi yang diizinkan dan paket yang tidak diizinkan melewati router.

Winbox adalah alat untuk akses jarak jauh ke *server proxy* dalam mode GUI, ketika *server proxy* dikonfigurasikan dalam mode teks dari komputer itu sendiri. Untuk mode GUI dengan *winbox*, Anda dapat mengkonfigurasi proxy dari komputer klien (Bumi et al., 2021).

3. METODOLOGI

Metode Simulasi berasal dari kata simulate yang artinya berbuat seakan-akan ada kejadian. Sebagai metode mengajar, simulasi dapat diartikan cara penyajian pengalaman belajar dengan mengguakan situasi tiruan untuk memahami tentang konsep, prinsip, atau keterampilan tertentu. Khususnya pada jaringan komputer terdapat metode simulasi yang digunakan untuk pembelajaran maupun proses penelitian.

Identification, Analysis, Design, Implement, Enforcement dan Enhancemen maka dari itu umpan balik dari evaluasi in bisa berdampak pada perubahan dalam arsitektur dan teknologi yang digunakan saat ini.

Adapun penjelasan tahap-tahap sebagai berikut :

1. *Identification*

Pada tahapan ini dilakukan proses identidikasi masalah yang dijadikan dasar dari jurnal-jurnal, dan buku untuk menjuang penelitian.

2. *Analysis*

Analisa Kebutuhan, tahap analisis dilakukan untuk mengumpulkan data yang dibutuhkan dalam penelitian. Pada tahap ini bertujuan untuk memperoleh informasi mengenai harapan dari pengguna sistem atau aplikasi yang akan dikembangkan.

3. *Design*

Desain Sistem, tahap desain dilakukan untuk membuat simulasi rancangan yang siap untuk diimplementasikan. Pada tahap ini akan dibuat rancangan sistem seperti arsitektur sistem.

4. *Implement*

Unit-unit individu program atau program digabung dan diuji sebagai sebuah sistem lengkap untuk memastikan apakah sesuai dengan kebutuhan perangkat lunak atau tidak.

5. *Enforcement*

Pengujian Program, setelah pengkodean selesai maka dilakukan tahap pengujian terhadap sistem yang sudah dikembangkan.

6. *Enhancement*

Hasil analisis untuk memahami perilaku sistem memberikan pemahaman yang lebih dalam menganalisis sistem yang sedang diteliti serta membatu dalam mengekplorasi data numerik yang dihasilkan oleh simulasi.

Gambar 1. Alur Penelitian

Gambar 1 merupakan alur penelitian yang diihunakan penulis dalam melakukan penelitian ini. Alur penelitian merupakan suatu alur diagram yang menjelaskan proses berjalannya sebuah penelian.

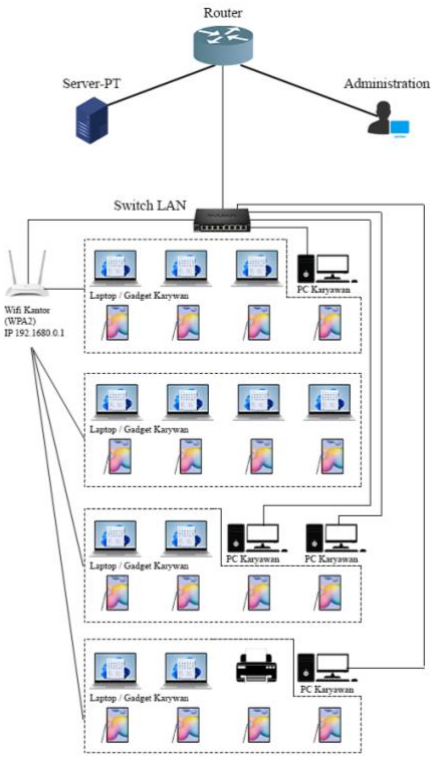
Pada tahap pembuatan sistem keamanan untuk mengamankan jaringan ada beberapa tahapan mulai dari identifikasi hingga melakukan pengujian sistem keamanan jaringan menggunakan *Firewall Rule*.

4. PEMBAHASAN

4.1. Identifikasi

Berdasarkan observasi pada instansi terdapat satu server dan jaringan internet yang terpasang dalam lingkup kantor tersebut memakai Wlan Ubiquiti unif U6-PRO *access point wifi* 6 dengan kecepatan maksimum hingga 9,6 Gbps, menggunakan topologi jaringan infrastrukrut dan keamanan jaringan yang diterapkan menggunakan WPA2 dengan karakteristik 802.11a Frekuensi 5 Ghz tidak terdapat penerapan *firewall rule* pada mikrotik sehingga jaringan yang terdapat pada penelitian penulis di skenariokan terhubung dengan jaringan internet yang memiliki resiko terhadap akses eksternal yang dapat merusak jaringan berupa serangan port scanning yang menyebabkan port port yang terbuka akan mudah dengan mudah disusupi oleh attacker dan implementasi topologi jaringan yang tidak aman dapat menyebabkan pengguna yang tidak valid mengakses dan mengelola jaringan lokal di perusahaan.

4.2. Analisa



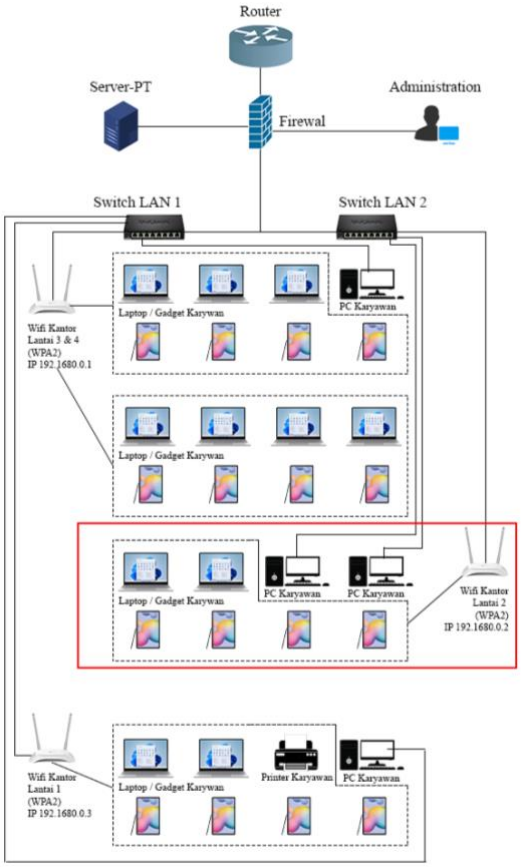
Gambar 2. Analisa Sistem Berjalan

Pada gambar 2, Sistem keamanan jaringan pada saat ini masih kurang efektif dan efisien dalam mensimulasikan tingkat keamanan pada jaringan internet, dimana keamanan jaringannya masih memiliki celah yang dapat disusupi dari pihak-pihak yang tidak memiliiki kewenangan. Solusi yang dapat diberikan penulis terkait dengan adanya ancaman keamanan jaringan komputer, berupa menambahkan *fitur firewall* pada *mikrotik* dengan menggunakan fitur *firewall rules*. Untuk mendeteksi dan mencegah ganguan serangan yang terjadi pada server yang terhubung di jaringan *wifi* dapat *capture* melalui aplikasi *wireshark*.

Penelitian ini memiliki dua jenis kebutuhan, yaitu kebutuhan fungsional dan kebutuhan non-fungsional. Kebutuhan fungsional adalah proses-proses yang akan dilakukan oleh sistem. Berikut alur kerja dari penelitian yang dilakukan:

1. Penelitian ini menggunakan sistem operasi *Windows 11* dan sistem operasi *Kali Linux Vmware 64bit*.
2. Penelitian ini melakukan serangan menggunakan 1 *client* pada jaringan *wifi*.
3. Pengujian dilakukan menggunakan 4 skenario, yaitu menggunakan *inSSIDer* untuk mengidentifikasi jaringan *wifi*, *Ettercap* untuk melihat aktifitas dari target yaitu *username* dan *password*, *nmap* untuk melihat *port-port* yang terbuka pada jaringan *wifi* dan *Low Orbit Ion Cannon* untuk mengirimkan paket yang banyak kepada target.
4. Sistem *Wireshark* dapat mencatat semua aktifitas serangan yang terjadi pada lalu lintas jaringan *wifi*.
5. fitur *firewall rules* dapat melakukan pembatasan aktifitas serangan.

4.3. Desain



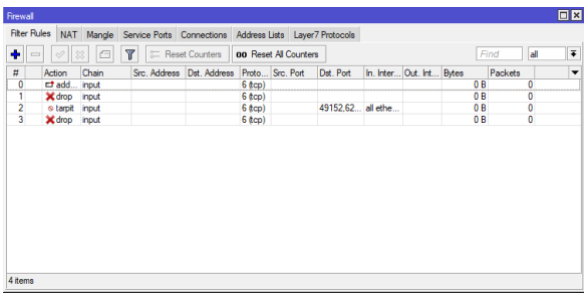
Gambar 3. Topologi Sistem yang diusulkan

Pada Gambar 3 adalah topologi sistem yang akan penulis usulkan saat proses implementasi. Pada topologi tersebut penulis akan menggunakan *wifi* kantor lantai 2 lalu penulis terhubung dengan jaringan yang sama dengan target untuk menyerang IP client.

IP public yang digunakan pada topologi diatas sewaktu-waktu dapat bisa berubah sesuaii dengan provider yang digunakan.

4.4. Implementasi

Pada tahapan ini menurut metode simulasi merupakan tahap lanjutan setelah proses identifikasi, analisa dan desain sistem yang telah dijabarkan sebelumnya. Peneliti akan menjelaskan mengenai aktivitas konfigurasi perangkat lunak, sistem operasi maupun sistem aplikasi yang digunakan pada penelitian.

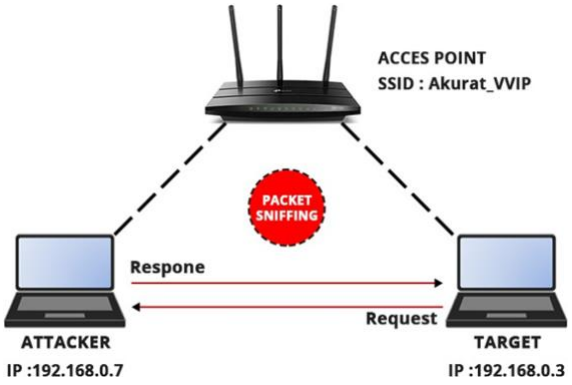


Gambar 4. Hasil Konfigurasi firewall rule

Pada gambar 4 adalah hasil konfigurasi *firewall rule* untuk melakukan penangkalan serangan dari serangan *packet sniffing*, *action drop* untuk melakukan *drop* terhadap ip yang terdeteksi oleh *action add* lalu *action tartip* untuk mengelabui *port* yang terbuka pada target.

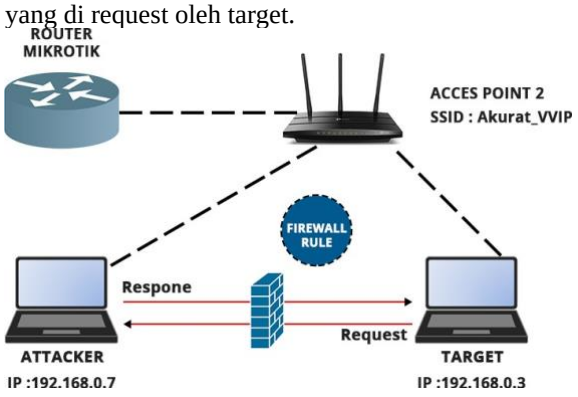
4.5. Pengujian

Pada tahapan ini, penulis melakukan 2 skenario yaitu serangan pada sistem keamanan jaringan *wifi* sebelum dilakukan *fitur firewall rules* dan serangan pada sistem keamanan jaringan *wifi* yang sudah dilapisi *fitur firewall rules*, apakah berhasil untuk mencegah dan merekam serangan yang terjadi pada jaringan *wifi*.



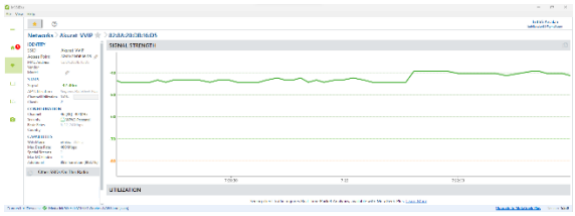
Gambar 5. Simulasi Penyerangan Sebelum di Beri Firewall Rule

Pada Gambar 5 menggambarkan ilustrasi ketika koneksi jaringan internet telah diretas oleh attacker berhasil menempatkan dirinya di tengah-tengah target dan router yang artinya setiap kali target melakukan *request* maka akan terlihat juga oleh *attacker* apa yang di request oleh target.



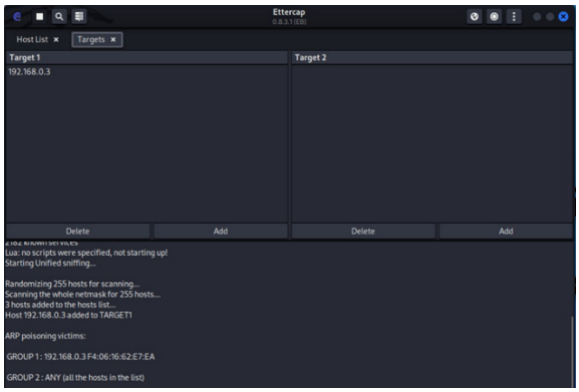
Gambar 6. Simulasi Penyerangan Sesudah di Beri *Firewall Rule*

Pada gambar 6 menggambarkan ilustrasi ketika koneksi jaringan internet telah diretas oleh *attacker* dan tidak berhasil menempatkan dirinya di tengah-tengah target dan *router* yang artinya setiap kali target melakukan *request* maka akan tidak terlihat oleh *attacker* apa yang di *request* oleh target karena sudah diberikan *firewall rule* pada router mikrotik.

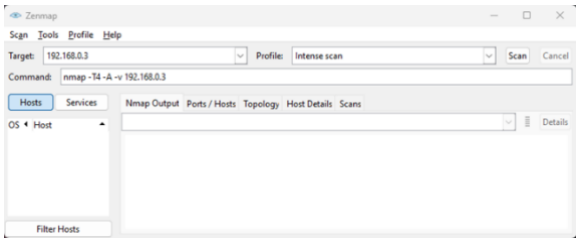


Gambar 7. Pengujian Identifikasi Wifi

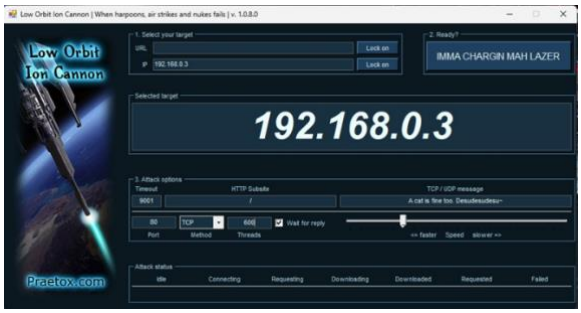
Pada gambar 7 Pengujian *software inSSIDer* pada *wifi* Akurat_VVIP dan pada Gambar 8 Pengujian serangan *arp spoofing* menyerang target dengan IP 192.168.0.3 menggunakan *tools Ettercap*. Selanjutnya Pengujian serangan menggunakan *tools Nmap* menyerang target dengan IP 192.168.0.3 seperti pada Gambar 9.



Gambar 8. Pengujian *Arp Spoffing*



Gambar 9 Pengujian *Port Scanning*



Gambar 10. Pengujian *Ddos Attack*

Langkah berikutnya, Pengujian serangan menggunakan tools Low Orbit Ion Cannon menyerang target dengan IP 192.168.0.3 mengirimkan paket tcp yang banyak pada computer target seperti yang terlihat pada gambar 10.

4.6. Hasil

Berikut ini adalah table hasil pengujian serangan *packet sniffing* pada jaringan *wifi* di PT Akurat Sentra Media.

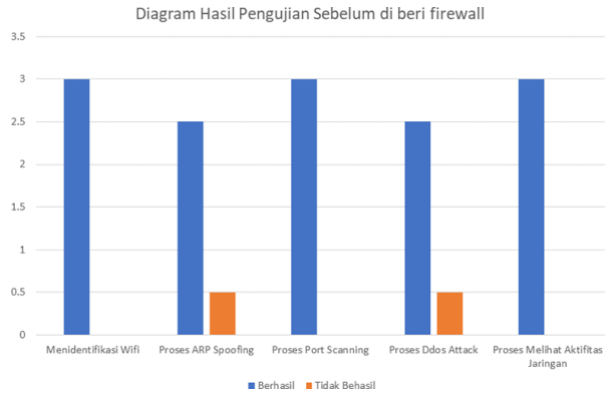
Tabel 2. Hasil Aktifitas *Packet Sniffing* sebelum di beri *firewall rule*

Aktivitas	Software	Ket.	Hasil
Mengidentifikasi *Wifi*	*InSSIDer*	Berhasil	Menampilkan nama SSID Akurat_VVIP, -Mac address 82:8A:20:DB:16:D5 - Channel 46 dan 48 -Security yang dipakai WP2A-Personal
Serangan *Arp Spoofing*	*Ettercap*	Berhasil	Mendapatkan username beserta password admin yaitu dari halaman login http:192.168.0.1 dengan username : akuratco dan password: adminakuratco12
Serangan *Port Scanning*	*Nmap*	Berhasil	Menampilkan port-port yang terbuka yaitu port 49152 dan 62078
Serangan *Ddos Attack*	*Low Orbit Ion Cannon*	Berhasil	Mengirimkan 600,800,1000,1200 dan 1500 paket tcp yang banyak ke komputer target
Proses Melihat Aktifitas Serangan	*Wireshark*	Berhasil	Menampilkan aktifitas jaringan yang dilakukan penyerang terhadap target.

Tabel 3. Hasil Aktifitas *Packet Sniffing* sesudah di beri *firewall rule*

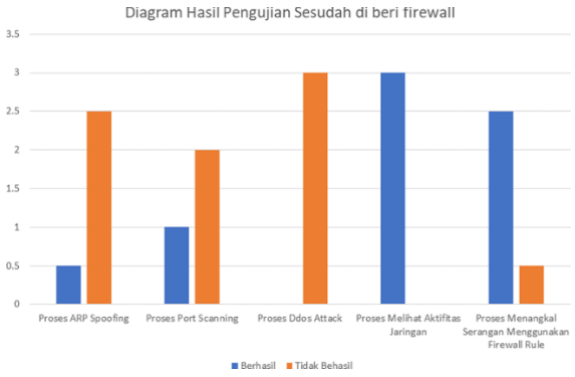
Aktivitas	Software	Ket.	Hasil
Serangan *Arp Spoofing*	*Ettercap*	Tidak Berhasil	Tidak berhasil melakukan sniffing ke target dan tidak mendapatkan username dan password admin
Serangan *Port Scanning*	*Nmap*	Tidak Berhasil	Menampilkan port yang terbuka tetapi port yang terbuka tersebut untuk mengelabui target seakan akan port tersebut terbuka
Serangan *Ddos Attack*	*Low Orbit Ion Cannon*	Tidak Berhasil	Tidak bisa mengirimkan paket yang banyak ke komputer target
Proses Melihat Aktifitas Serangan	*Wiresharak*	Berhasil	Menampilkan aktifitas jaringan yang dilakukan penyerang terhadap target
Proses Menangkal Serangan Menggunakan *Firewall Rule*	*Winbox*	Berhasil	Fitur *Firewall Rule* yang tersedia pada *winbox* berhasil menangkal serangan *packet sniffing* yaitu serangan - *arp spoofing* - *port scanning*

Aktivitas	Software	Ket.	Hasil
			- *ddos attack*



Gambar 11. Diagram hasil pengujian sebelum di beri firewall rule

Gambar 11 menunjukkan hasil pengujian seraangan *packet sniffing* sebelum diberi *firewall rule* dilakukan masing-masing 5 kali serangan, dapat diketahui bahwa dengan melakukan identifikasi memiliki skala yang tinggi, proses serangan arp spoofing berhasil melakukan 4 serangan dan 1 kegagal hasil tersebut memiliki skala yang cukup baik, proses serangan port scanning berhasil mekakukan 5 scanning hasil memiliki skala yang baik, proses serangan ddos attack berhasil melakukan 4 serangan dan 1 kegagalan hasil tersebut memiliki skala yang cukup baik dan proses melihat aktifitas serangan *packet sniffing* memiliki skala yang tinggi.



Gambar 12. Diagram hasil pengujian setelah di beri *firewall rule*

Gambar 12 menunjukkan hasil pengujian serangan *packet sniffing* setelah diberi *firewall rule* dilakukan masing- masing 5 kali serangan, dapat diketahui bahwa dengan melakukan proses serangan arp spoofing setelah diberi *firewall rule* berhasil melakukan 4 penangkalan terhadap serangan dan 1 kegagalan hasil tersebut memiliki skala yang cukup baik proses serangan port scanning setelah diberi *firewall rule* berhasil melakukan 5 kali penangkalan terhadap scanning port hasil tersebut memiliki skala yang cukup baik, proses serangan ddos attack setelah diberi *firewall rule* berhasil melakukan 5 penangkalan terhadap serangan hasil tersebut memiliki skala yang baik, proses melihat aktifitas serangan *packet sniffing* memiliki skala yang tinggi dan proses mengkal semua seranga *packet sniffing* setelah menggunakan *firewall rule* memiliki skala cukup baik.

5. KESIMPULAN DAN SARAN

Bedasarkan hasil pembahasan peneliti yang telah penulis lakukan, diperoleh kesimpulan bahwa, Identifikasi dilaukan menggunakan fitur SSID, *mac address*, *channel* dan *security* yang dipakai WP2A-Personal pada jaringan *wifi* di PT Akurat Sentra Media. Pengujian sebelum dilakukan penerapn fitur *firewall rule* terhadap *wifi* berhasil menyerang *wifi* dengan rata-rata 4 skala dan pengujian sesudah dilakukan fitur *firewall rule* berhasil menanggkal serangan dengan rata-rata skala 4,5. Menerapkan *loss-of-functions* ke *router* memiliki dampak positif pada jaringan, karena menyulitkan penyerang untuk menyebarkan atau membanjiri paket dengan cara yang dapat menyebabkan gangguan jaringan dan putusnya koneksi

Pemeriksaan jaringan secara berkala diperlukan untuk menghindari terjadinya permasalahan pada jaringan yang dapat menyebabkan menurunnya kualitas jaringan. Pada penelitian kali ini kita mengguunakan *software InSSDer*, *Ettercap*, *Nmap*, *Loic dan Wireshark* sebagai *tools* penyerangan dan dapat diteruskan pada penelitian selanjutnya menggunakan *tools packet sniffing* yang lain. Pada penelitian selanjutnya menggunaan percobaan serangan lain. Pada penelitian selanjutnya disarankan untuk menggunakan *software* atau *hardware* yang lain untuk mengantisipasi serangan *packet sniffing*. Pada penelitian selanjutnya diharapkan lebih mempersiapkan diri dalam proses pengambilan dan pengumpulan dan segala sesuatunya sehingga penelitian dapat dilaksanakan dengan lebih baik.

DAFTAR PUSTAKA

Al Fikri, K. and Djuniadi, D., 2021. Keamanan Jaringan Menggunakan Switch Port Security. InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 5(2), pp.302–307.

Amarudin, A., 2018. Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik Router Os Menggunakan Metode Port Knocking. Prosiding Semnastek.

Ariyadi, T., 2018. Mitigasi Keamanan Dynamic Host Control Protocl (DHCP) Untuk Mengurangi Serangan Pada Local Area Network (LAN). INOVTEK Polbeng-Seri Informatika, 3(2), pp.147–154.

Dharma, S. and Thamrin, T., 2020. Analisis Kinerja Jaringan WIFI. Voteteknika (Vocational Teknik Elektronika Dan Informatika), 8(2), pp.35–42.

Febriyanti Panjaitan, Y., 2022. Hijacking Session Terhadap Sistem Informasi Akademik Universitas Islam Negeri Raden Fatah

Palembang. Hijacking Session Terhadap Sistem Informasi Akademik Universitas Islam Negeri Raden Fatah Palembang.

Gunawan, I., 2021. Analisis Keamanan Jaringan Wifi Menggunakan Wireshark. JES (Jurnal Elektro Smart), 1(1), pp.10–12.

Gustiawan, M., Yudianto, R.J., Pratama, J. and Fauzi, A., 2021. Implementasi Jaringan Hotspot Di Perkantoran Guna Meningkatkan Keamanan Jaringan Komputer. Jurnal Nasional Komputasi dan Teknologi Informasi, 4(4), pp.244–247.

Hae, Y., 2021. Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen. JATISI (Jurnal Teknik Informatika dan Sistem Informasi), 8(4), pp.2095–2105.

Hariyadi, D., Kusuma, M., Sholeh, A. and Fazlurrahman, 2021. Digital Forensics Investigation on Xiaomi Smart Router Using SNI ISO/IEC 27037:2014 and NIST SP 800-86 Framework. [online] International Conference on Science and Engineering (ICSE-UIN-SUKA 2021). Atlantis Press. pp.143–147. https://doi.org/10.2991/aer.k.211222.023.

I Dewa Made Bayu Atmaja Darmawan and I Gede Oka Gatria Atitama, 2021. Modul Workshop Mikrotik Fundamental. Teknik Informatika UNIVERSITAS UDAYANA.

Jan William Tarigan, J., 2019. SCANNING DAN VULNERABILITY MENGGUNAKAN NMAP, NIKTO, DAN SPARTA. unsri. [online] Available at: <http://edocs.ilkom.unsri.ac.id/id/eprint/3493>.

Junita, R., SANDI, D., SEPTIAWAN, V. and TOBING, T., 2013. Infrastruktur Jaringan Wi-Fi (Wireless Fidelity) Universitas Dian Nuswantoro Semarang. KKP MAHASISWA TI S1.

Marta, I.K.K.A., Hartawan, I.N.B. and Satwika, I.K.S., 2020. Analisis Sistem Monitoring Keamanan Server Dengan Sms Alert Berbasis Snort. INSERT: Information System and Emerging Technology Journal, 1(1), pp.25–40.

Pranata, H., Abdillah, L.A. and Ependi, U., 2015. Analisis Keamanan Protokol Secure Socket Layer (SSL) Terhadap Proses Sniffing di Jaringan. arXiv preprint arXiv:1508.05457.

Riyanto, S., Rahmat, R. and Zulfachmi, Z., 2021. Penempatan Access Point Pada Jaringan Wi-Fi di Sekolah Tinggi Teknologi Indonesia Tanjungpinang. Jurnal Bangkit Indonesia, 10(2), pp.27–31.

Rizkiyani, 2020. Analisis Keamanan Jaringan Pada Fasilitas Internet(Wifi) Terhadap Serangan Packet Sniffing Di Kantor Koran Seruya. [online] Available at: <https://dokumen.tips/documents/analisis-keamanan-jaringan-pada-fasilitas-.html?page=1> [Accessed 10 December 2023].

Suherdi, D., 2021. Pemanfaatan Firewall Pada Jaringan Mengunankan Mikrotik RB951Ui–2HnD. Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD, 4(2), pp.173–179.

Tri Novita, R., Gunawan, I., Marleni, I. and Gregarius Grasia, O., 2019. Nanda Valentika abcde Teknik Elektro Sekolah Tinggi Teknologi Ronggolawe Cepu Penulis Korenspondensi, M.(2021). Analisis Keamanan Wifi Menggunakan Wireshark. JES(Jurnal Elektro Smart), 1(1), pp.7–9.