Jurnal Nasional Teknologi Komputer
Vol.5; No: 3; Juli 2025
Website: publikasi.hawari.id/index.php/jnastek
E-ISSN: 2808-4845; P-ISSN: 2808-7801

Penerapan Secure Coding Sebagai Cyber Security Based Pada PT. Industri Karet Deli

Denny Ramahdana[1], Zuhri Ramadhan[2]

[1,2]Sistem Komputer, Sains dan Teknologi, Universitas Pembangunan Panca Budi
[1]dennyramahdana24@gmail.com, [2]ramadhanzoe@pancabudi.ac.id

Corresponding Author: Denny Ramahdana

ABSTRACT

Cyber security is a crucial aspect in maintaining the integrity, confidentiality, and availability of a company's information systems. PT. Industri Karet Deli, as one of the national manufacturing companies that has implemented digital systems in its operations, faces significant challenges in terms of potential cyber threats. This study aims to apply secure coding principles as the basis for strengthening cyber security systems. The methods used include identifying security vulnerabilities in the company's internal applications, evaluating the source code, and implementing secure coding practices in accordance with OWASP (Open Web Application Security Project) standards. The research results show that the systematic implementation of secure coding can reduce system vulnerabilities by up to 60% compared to before implementation. These findings emphasize the importance of integrating security from the early stages of software development to create systems that are resilient to cyber attacks. Recommendations from this study include regular training for development teams and the adoption of code review policies as part of the continuous system development process.

Keywords: Secure Coding, Cyber Security, OWASP, Information Systems, PT. Deli Rubber Industry

ABSTRAK

Keamanan siber merupakan aspek krusial dalam menjaga integritas, kerahasiaan, dan ketersediaan sistem informasi perusahaan. PT. Industri Karet Deli sebagai salah satu perusahaan manufaktur nasional yang telah mengimplementasikan sistem digital dalam operasionalnya, menghadapi tantangan besar terhadap potensi ancaman siber. Penelitian ini bertujuan untuk menerapkan prinsip *secure coding* sebagai dasar dalam penguatan sistem keamanan siber (*cyber security based*). Metode yang digunakan meliputi identifikasi celah keamanan pada aplikasi internal perusahaan, evaluasi terhadap kode sumber (*source code*), serta penerapan praktik *secure coding* sesuai dengan standar OWASP (Open Web Application Security Project). Hasil penelitian menunjukkan bahwa penerapan *secure coding* secara sistematis mampu menurunkan potensi kerentanan sistem hingga 60% dibandingkan sebelum penerapan. Temuan ini menegaskan pentingnya integrasi keamanan sejak tahap awal pengembangan perangkat lunak guna menciptakan sistem yang tangguh terhadap serangan siber. Rekomendasi dari penelitian ini mencakup pelatihan berkala bagi tim pengembang dan pengadopsian kebijakan *code review* sebagai bagian dari proses pengembangan sistem yang berkelanjutan.

Kata kunci: Secure Coding, Cyber Security, OWASP, Sistem Informasi, PT. Industri Karet Deli

1. Pendahuluan

Pendistribusian akses jaringan menggunakan teknologi nirkabel atau *wireless* saat ini semakin menjadi pilihan. Cakupan area, kemudahan serta sifat *flexible* pada *wireless* menjadi alasan admin jaringan menggunakan nya. Untuk area-area yang banyak dikunjungi orang seperti mal, cafe, atau kantor dimana pengunjung akan selau berganti dengan jumlah yang tidak tentu (dinamis), teknologi *wireless* sangat tepat digunakan. Dalam implementasi di lapangan,

sebelum perangkat *wireless* Mikrotik dapat memberikan akses ke *client* di bawah nya, maka perangkat tersebut harus dapat menerima akses dari provider terlebih dahulu.

Ada 2 metode yang bisa digunakan dalam melakukan distribusi wireless ke arah client. Pertama dengan topologi point to point dan yang kedua adalah point to multipoint. Pada wireless Mikrotik ada banyak mode yang dapat digunakan untuk membangun jaringan wireless. Biasa digunakan untuk pendistribusian akses ke arah perangkat wireless lain, misal dari NOC ke arah BTS atau dari NOC ke arah client dengan jarak cukup jauh, dimana client tidak bisa menangkap pancaran frekuensi NOC secara langsung. Untuk dapat membangun jaringan point to point, pada perangkat Mikrotik dibutuhkan minimal Router OS Lisensi Level 3, baik di sisi AP maupun Station. Pada umunya dalam topologi ini perangkat wireless hanya digunakan untuk bridging saja, sedangkan service dan manajemen langsung dilakukan di Router Utama.

Transformasi digital di industri manufaktur membawa tantangan baru dalam bentuk risiko keamanan sistem informasi. PT. Industri Karet Deli, sebagai perusahaan berbasis manufaktur, mulai mengadopsi sistem digital dalam berbagai aspek operasionalnya. Namun, kurangnya perhatian terhadap praktik *secure coding* menyebabkan sistem perusahaan rentan terhadap serangan siber. Oleh karena itu, penelitian ini bertujuan menerapkan prinsip *secure coding* untuk memperkuat sistem keamanan siber perusahaan.

2. Tinjauan Pustaka

2.1. Jaringan Komputer

Konsep jaringan komputer lahir pada tahun 1940-an di Amerika dari sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan group riset Harvard University yang dipimpin profesor Howard Hathaway Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (Batch Processing), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan kaidah antrian. Ditahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, maka sebuah komputer mesti melayani beberapa terminal. Christpoher Strachy di tahun 1959 memberikan ide berkaitan dengan pembagian waktu yang dilakukan oleh CPU. setiap user akan diberikan layanan oleh komputer secara bergantian dalam waktu yang singkat. Untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (Time Sharing System) , maka untuk pertama kali bentuk jaringan (network) komputer diaplikasikan.

Time sharing system atau yang biasa disingkat TSS merupakan sebuah teknik yang digunakan di dalam penggunaan online sistem ada beberapa pengguna secara bergantian berdasarkan waktu yang dibutuhkan. Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah host komputer. Dalam proses TSS mulai nampak perpaduan teknologi komputer dan teknologi telekomunikasi yang padaawalnya berkembang sendiri-sendiri. Memasuki tahun 1970-an, setelah beban pekerjaan bertambah banyak dan harga perangkat komputer besar mulai terasa sangat mahal, maka mulailah digunakan konsep proses distribusi (Distributed Processing). Dalam proses ini beberapa host komputer mengerjakan sebuah pekerjaan besar secara paralel untuk melayani beberapa terminal yangtersambung secara seri disetiap host komputer. Dalam proses distribusi sudah mutlak diperlukan perpaduan yang mendalam antara teknologi komputer dan telekomunikasi, karena selain proses yang harus didistribusikan,

semua host komputer wajib melayani terminal-terminalnya dalam satu perintah dari komputer pusat.

Jaringan komputer adalah sebuah sistem yang terdiri dari perangkat komputer dan jaringan yang didesain untuk dapat berbagi sumber daya dan dapat mengakses informasi. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*). Pihak yang menerima layanan disebut klien (*client*) dan yang memberikan layanan disebut pelayan (*server*). Desain ini disebut dengan sistem *client-server*, dan digunakan pada hampir seluruh sistem jaringan komputer."(Syafrizal, 2014 : 2). Dalam sebuah jaringan komputer biasanya terdiri dari dua atau lebih komputer yang saling berhubungan satu sama lain dan saling berbagi sumber daya, misalnya *CD ROM, printer, scanner,* pertukaran *file* bahkan berkomunikasi secara elektronik. Komputer yang terhubung, dimungkinkan berhubungan dengan media kabel, saluran telepon, gelombang radio, satelit, sinar *infra merah*, atau tanpa kabel.

Topologi jaringan sendiri adalah suatu cara / konsep yang digunakan untuk menghubungkan dua komputer atau lebih, berdasarkan hubungan geometrisantara unsur-unsur dasar penyusun jaringan, yaitu node, link, dan station. Pemilihan topologi jaringan didasarkan pada skala jaringan, biaya, tujuan, danpengguna. Topologi pertama kali yang digunakan adalah topologi bus.

2.2. Network Layer

Network layer Merupakan layer ketiga pada model referensi OSI layer. Network layer, merupakan layer yang mendefinisikan akhir pengiriman paket data dimana komputer mengidentifikasi logical address seperti IP Addreses, bagaimana meneruskan/routing (oleh router) untuk siapa pengiriman paket data. Layer ini juga mendefinisikan fragmentasi dari sebuah paket dengan ukuran unit yang lebih kecil. Sehingga Tugas utama lapisan jaringan adalah menyediakan fungsi routing, sehingga paket dapat dikirim keluar dari segment network local ke suatu tujan yangberbeda pada suatu network lain.

Fungsi utama dari layer tiga, yaitu layer Network adalah pada referensi model OSI untuk enable message untuk melewati antar jaringan local yang terhubung, yang biasanya lebih banyak jaringan lewat link WAN. Piranti-piranti, protocol-protocol,dan programprogram yang berjalan pada layer Network bertanggung jawab untuk mengidentifikasikan, memilah, dan mengarahkan traffic yang melalui antar- jaringan. Jaringan menjelaskan beberapa kumpulan dari piranti terhubung bersama-sama untuk berbagi informasi dan resources dan juga saling berkomunikasi. Secara fisik, jaringan diidentifikasikan oleh segmen-segmen media transmisi dan juga oleh address-address jaringan.

Subnetting adalah teknik memecah network (jaringan komputer) menjadi beberapa subnetwork yang lebih kecil. Subnetting hanya dapat dilakukan pada IP Address kelas A, kelas B, dan Kelas C saja. Dan dengan teknik subnetting, maka suatu network dapat menciptakan beberapa network tambahan, tetapi hal itu sayangnya bisa mengurangi jumlah maksimum host yang ada dalam tiap network tersebut. Secara sederhana, subnetting itu sama halnya dengan analogi sebuah jalan. Misalnya, Jalan Gatot Subroto terdiri dari beberapa rumah bernomor 01-08. Dan rumah bernomor 08 adalah rumah ketua RT yang memiliki tugas untuk mengumumkan informasi apapun kepada seluruh rumah yang ada di wilayah jalan Gatot Subroto tersebut. Kemudian, ketika rumah di wilayah itu semakin banyak, pastinya hal tersebut akan menimbulkan kemacetan dan hal-hal buruk merepotkan lainnya. Karena itulah kemudian rumah-rumah baru tersebut akan diatur lagi, seperti dibuat gang-gang, diberi nomor rumah, dan

setiap gang memiliki ketua RT-nya masing-masing. Upaya tersebut tentunya untuk memecahkan kemacetan, efiesiensi, dan optimalisasi transportasi. Serta ketua RT dalam hal ini berperan sebagai previledge untuk mengelola wilayahnya masing-masing di setiap gang. Sebenarnya seperti itu pulalah cara kerja Subnetting. Namun Subnetting bukan berupa jalan, tapi berupa network (jaringan komputer). Dalam artian untuk memudahkan pengoptimalisasian jaringan komputer dalam suatu lembaga, kantor, atau hal-hal lainnya yang rasanya perlu untuk di subnetting.

Subnet mask adalah istilah teknologi informasi yang fungsinya untuk membedakan network id dan host id atau sebagai penentu jumlah network id dan host id pada deretan kode biner. selain membedakan network id dengan host id, subnet mask juga berfungsi untuk menentukan alamat tujuan paket data. apakah pengiriman data berupa local atau remote.

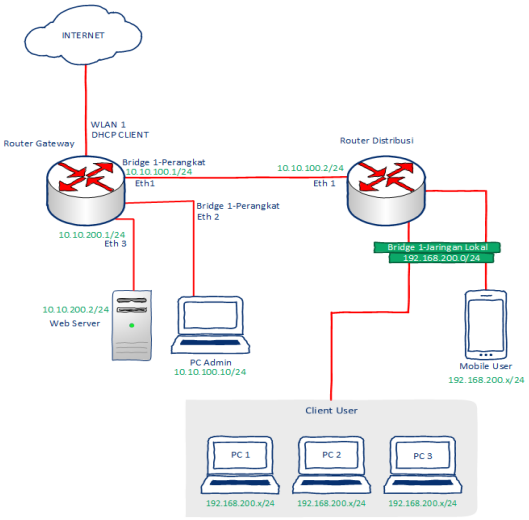
2.3. Routing

Routing adalah suatu protokol yang digunakan untuk mendapatkan rute darisatu jaringan ke jaringan yang lain. Rute ini, disebut dengan route dan informasi route secara dinamis dapat diberikan ke router yang lain ataupun dapat diberikan secara statis ke router lain. Seorang administrator memilih suatu protokol routing dinamis berdasarkan keadaan topologi jaringannya. Misalnya berapa ukuran dari jaringan, bandwidth yang tersedia, proses power dalam router, merek dan model dari router, dan protokol yang digunakan dalam jaringan. Routing adalah proses dimana suatu router mem-forward paket ke jaringan yang dituju. Suatu router membuat keputusan berdasarkan IP address yang dituju oleh paket. Semua router menggunakan IP address tujuan untuk mengirim paket. Agar keputusan routing tersebut benar, router harus belajar bagaimana untuk mencapai tujuan. Ketika router menggunakan routing dinamis, informasi ini dipelajari dari router yang lain. Ketika menggunakan routing statis, seorang network administrator mengkonfigurasi informasi tentang jaringan yang ingin dituju secara manual. Default route adalah sebuah rute yang dianggap cocok dengan semua IP address tujuan. Dengandefault route ketika IP address destination(tujuan) dari sebuah paket tidak ditemukan dalam tabelrouting, maka router akan menggunakan defaultroute untuk mem-forward paket tersebut.

3. Bahan & Metode

3.1. Topologi Jaringan

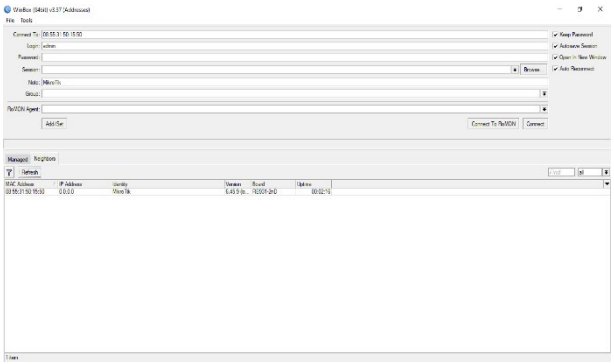
Berikut adalah rancangan topologi yang digunakan.



3.2. Rancangan Pengaturan Winbox

Berikut ini merupakan tampilan pada aplikasi winbox pada tab menu Neighbors. Pada tab ini akan muncul mac address perangkat router yang terkoneksi. Kemudian untuk melakukan remote dan melakukan konfigurasi router, Langkahnya sebagai berikut:

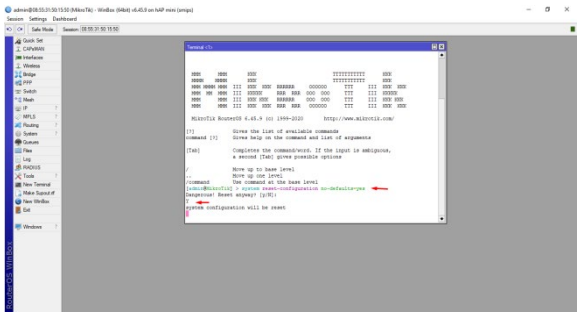
a. Apabila menggunakan router yang baru dari toko, pastikan untuk menghubungkan kabel UTP atau kabel LAN pada port 2 router agar lebih mudah untuk dilakukan nya remote router. Karena jika di hubungkan ke port 1 router, kita diharuskan untuk melakukan konfigurasi IP Static dari subnet IP (192.168.88.X/24) pada PC agar dapat meremote router, karena pada port 1 masih terdapat default konfigurasi pabrik.
b. Pastikan kabel UTP terhubung pada PC Admin dan Mac address router terdeteksi.
c. Klik Mac Address
d. Login Menggunakan username : admin , password : (tanpa password)



Sebelum melakukan konfigurasi lebih lanjut pada router, terlebih dahulu harus melakukan reset default konfigurasi pada router yakni dengan cara sebagai berikut:

1. Buka New Terminal
2. Ketikan perintah system reset-configuration no-defaults=yes
3. Enter
4. Ketik Y

Tunggu sampai router selesai restart, kemudian login kembali



3.3. Konfigurasi Router Gateway

3.3.1. Pemberian Identitas Router Gateway

Agar router mudah dikenali dan untuk memudahkan melakukan maintenance dan troubleshooting maka sebuah router harus diberikan Identitas, caranya sebagai berikut:

1) Pilih menu system
2) Pilih Identity
3) Kemudian pada kolom Identity berikan nama router sesuai kebutuhan
4) Klik Apply kemudian OK

3.3.2. Penambahan Users Login Router Mikrotik

Penambahan users untuk login router merupakan salah satu langkah untuk mengamankan router. Langkahnya sebagai berikut :

1) Pilih menu system
2) Pilih users
3) Klik Add dengan symbol (+)
4) Kemudian isikan username dan password yang unik
5) Pilih Group : Full
6) Klik Apply lalu OK

Sebelum menghapus user default (admin), pastikan terlebih dahulu berhasil login dengan users yang baru ditambahkan.

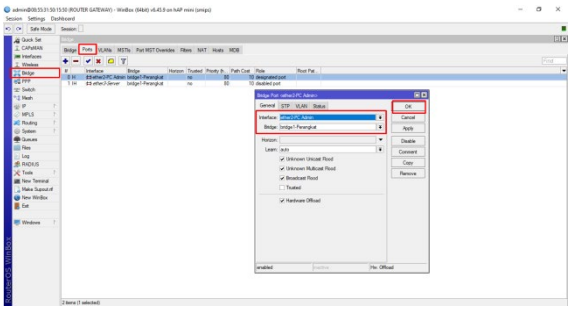
3.3.3. Pengaturan Waktu pada Router Mikrotik

Pengaturan waktu pada router sangat berfungsi menjelaskan keterangan waktu pada Log router. Berikut ini langkahnya:

1) Pilih menu system
2) Pilih Oclock
3) Kemudian atur waktu yang sesuai
4) Klik apply
5) Klik OK

3.4. Penambahan Interface Bridge

Pada topologi ini perangkat router dan pc admin ada dalam satu subnet, yaitu Eth1 terhubung ke pc router distribusi dan Eth2 terhubung ke perangkat pc admin. Maka dibutuhkan 1 buah interface bridge yang dapat menggabungkan kedua interface tersebut menjadi satu subnetting.



3.5. Pengaturan Interfaces Router Mikrotik

Untuk mempermudah identifikasi kabel UTP yang terhubung dari perangkat seperti server, pc, access point,switch dan lainnya menuju port pada router sebaiknya setiap interface yang digunakan diberi nama

3.6. Pengaturan Wireless Mode Station

Fungsi wireless selain sebagai pemancar sinyal (mode access point), wireless pada topologi ini digunakan sebagai penerima sinyal (mode station), karena pada topologi ini menggunakan Teathering Hotspot dari perangkat LTE/Handphone sebagai sumber internet. Berikut ini cara konfigurasinya :

1) Pilih menu Wirelless
2) Pilih tab menu Security Profiles
3) Tambahkan sebuah Security Profile dengan klik Add (+)
4) Pilih tab menu general
5) Isikan parameter berikut:
   a) Name: (cth:profile1)
   b) Centang semua Authentication Types
   c) WPA Pre-Shared-Key : (Isikan sesuai dengan password Teahering Hotspot dari LTE/Handpone)
6) Klik apply, kemudian OK
7) Selanjutnya Pilih tab menu WIFI Interfaces
8) Double klik Interface wlan1
9) Pilih tab menu wireless
10) Pilih Advances Mode
11) Pada parameter mode pilih station
12) Pada parameter security profile pilih profile yang dibuat sebelumnya (cth:profile1)
13) Pilih Scan
14) Pada parameter interface pilih wlan1
15) Klik Start
16) Pilih SSID dari Teathering LTE/Hanphone (cth:Corner Kick)
17) Klik Connect
18) Klik Apply, kemudian OK
19) Pastikan pada interface wlan1 sudah muncul flag “R” yang artinya Running

3.7. Pengaturan IP DHCP Client

Setelah wireless ditambahkan dengan mode station, selanjutnya harus ditambahkan IP address berdasarkan IP address yang digunakan dari Teathering LTE/Handphone agar dapat berkomunikasi ke internet.

3.8. Pengaturan IP Address

Untuk dapat berkomunikasi dengan router distribusi dan perangkat server yang ada dibawah router gateway ini, Maka interface Eth1 dan interface Bridge1-Perangkat harus ditambahkan IP.

3.9. Penambahan Static Routing

Routing static sangat berguna untuk menyatukan jaringan yang berbeda subnet sehingga dapat bertukar data dan berkomunikasi secara aman. Routing static tentu lebih aman dibanding dengan routing dinamic karena tabel routing dimasukan secara manual oleh administrator. Karena pada topologi diatas menggunakan subnet IP yang berbeda, maka dibutuhkan static routing

3.10. Pengaturan DNS

Pada router mikrotik terdapat pengaturan DNS (domain name system). DNS di mikrotik berfungsi sebagai penerjemah alamat domain ke IP address, karena sebenarnya pengalamatan di jaringan menggunakan IP address. DNS server yang bertujuan melayani request DNS dari client.

3.11. Pengaturan Firewall NAT

NAT merupakan singkatan dari Network Address Translation merupakan salah satu fungsi pada firewall yang digunakan untuk melakukan pengubahan IP Address pengirim maupun penerima dari sebuah paket data. Terdapat 2 tipe NAT, yakni Source NAT (srcnat) dan Destination NAT (dstnat). Fungsi lain dari Nat adalah sebagai sebuah manajemen pemetaan alamat IP dimana perangkat jaringan komputer akan meminjamkan alamat IP public kepada perangkat jaringan lokal agar banyak IP private yang dapat terhubung dengan jaringan public.

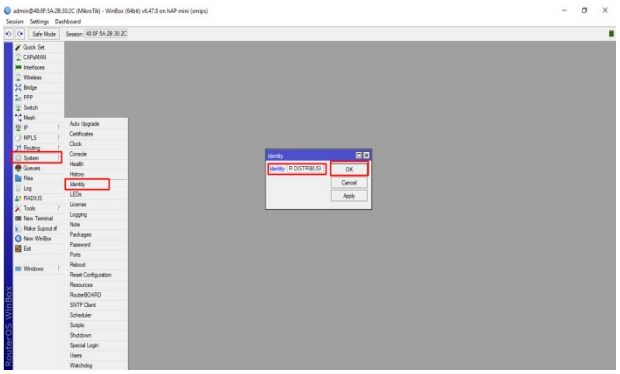
3.12. Pengaturan IP Static Client User

Untuk melakukan blokir pada perangkat yang akan mengakses ke sebuah perangkat server. Perangkat tersebut harus terlebih dulu ditandai saat terkoneksi ke router agar IP address perangkat tersebut tidak berubah saat ditambahkan rule pada firewall router untuk blokir dan rule dapat berjalan sesuai dengan kebutuhan. Salah satu cara menandai perangkat yang akan di blokir yaitu dengan menjadi ip perangkat tersebut menjadi static.

3.13. Konfigurasi Router Distribusi

Seperti pada router gateway sebelumnya, setiap router sebaiknya diberi identitas yang sesuai agar lebih mudah untuk penanganan jika terjadi masalah. Berikut langkah konfigurasi nya :

1) Pilih menu system
2) Pilih Identity
3) Isikan identitas router sesuai kebutuhan
4) Klik Apply, lalu OK



3.13. Pengaturan Service DHCP-Server pada Router Distribusi

Dhcp-Server merupakan sebuah layanan pada mikrotik yang memberikan dan mengatur pembagian alamat IP kepada pengguna secara otomatis. Selain IP address, server juga akan mengirimkan default Gateway, netmask, NTP server, dan IP DNS.

3.14. Penambahan Rule Firewall

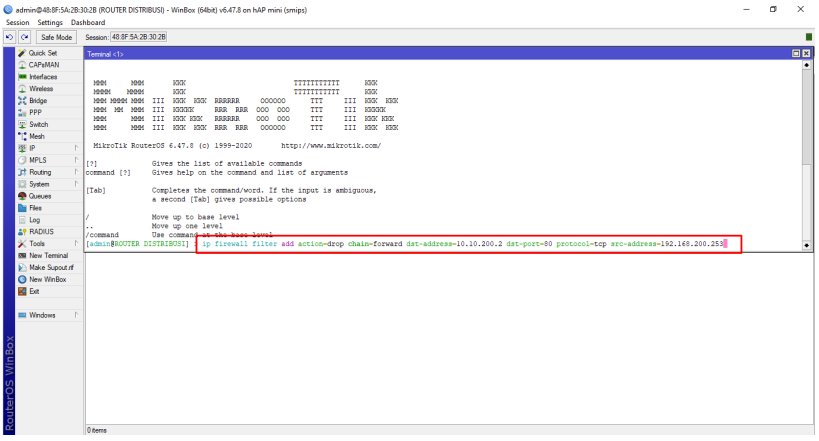
Untuk melakukan blokir menuju sebuah perangkat server, maka harus ditambahkan sebuah rule firewall pada router, agar perangkat client yang tidak diberikan izin akses web server tidak bsa melakukan komunikasi dengan server tersebut. Berikut ini adalah langkah penambahan rule firewall tersebut

1) Pilih menu New Terminal

2) Ketikan perintah berikut

```
/ip firewall filter add action=drop chain=forward dst-address=10.10.200.2 dst-port=80 protocol= tcp src-address=192.168.200.253
```

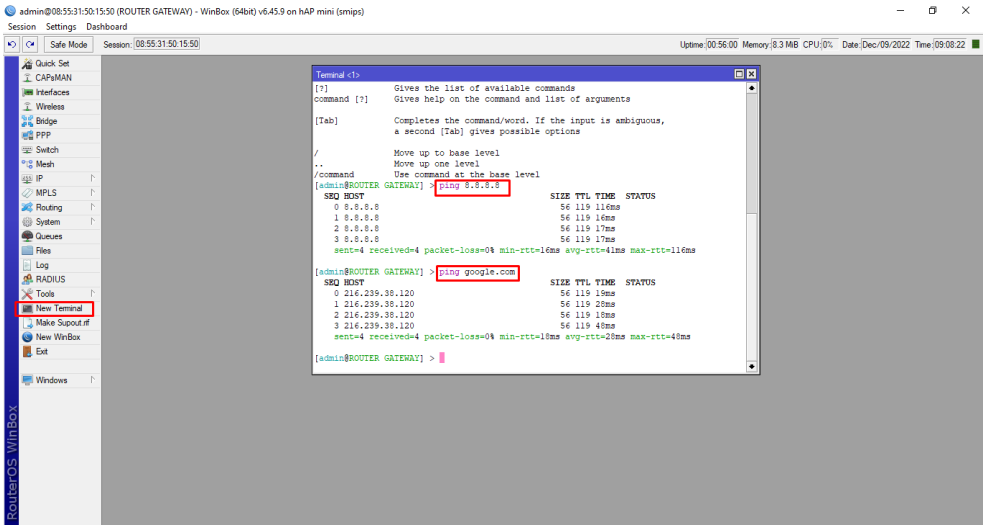
3) Enter



4. Hasil

4.1. Pengujian Koneksi Router ke Internet

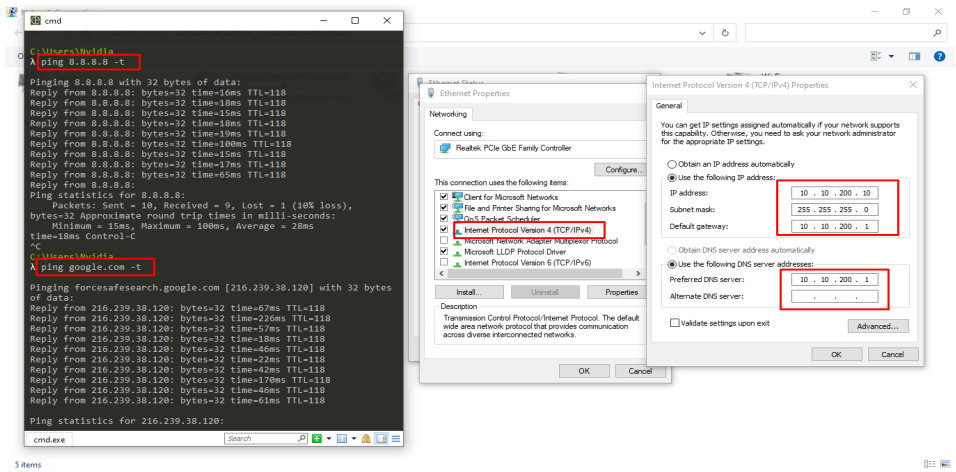
Setelah wireless mode station sudah mendapt IP dhcp dari Teathering LTE/Handphone, selanjutnya koneksi router ke internet harus di ujicoba terlebih dahulu dengan cara membuka menu New Terminal kemudian ketikan perintah ping 8.8.8.8 atau ping google.com , lalu tekan enter. Pastikan hasil ping tersebut Reply yang artinya router sudah dapat berkomunikasi ke internet.



Gambar 4.1 Pengujian Koneksi Route

4.2. Pengujian Koneksi Client ke Internet

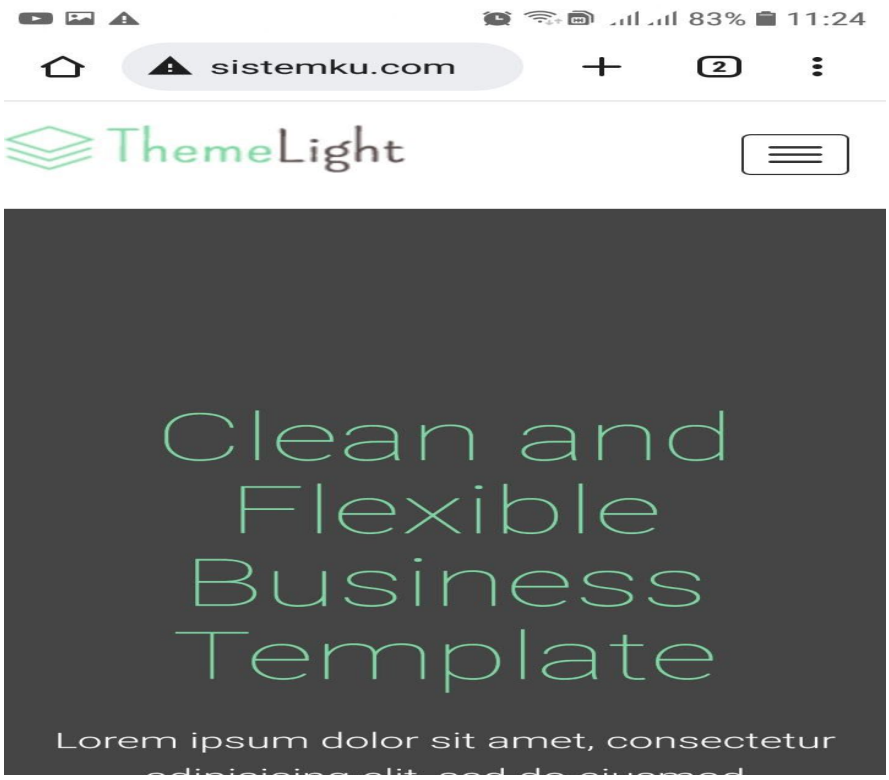
Setelah ip address sudah ditambahkan ke port router,penambahan DNS serta pengaturan firewall NAT. Kemudian perangkat client dengan melakukan pengujian koneksi perangkat client ke internet. Dengan menambah ip pada pengaturan perangkat sesuai dengan topologi kemudian melakukan tes ping ke ip dan dns google.



Gambar 4.2 Pengujian Koneksi Perangkat Client ke Internet

4.3. Pengujian Akses Web Server Sebelum Penambahan Firewall

Sebelum menambahkan sebuah rule pada firewall terlebih dahulu harus memastikan web server dapat diakses, agar terlihat perbedaan sebelum dan setelah penambahan rule firewall pada router untuk blokir akses menuju web server.



Gambar 4.3 Pengujian Akses Web Server

Audit awal menemukan 12 jenis kerentanan kritis, termasuk SQL Injection dan Broken Access Control. Setelah penerapan *secure coding*, 80% celah dapat ditutup. Penurunan risiko direfleksikan melalui pengujian penetrasi yang lebih baik. Selain itu, developer menunjukkan peningkatan pemahaman keamanan sebesar 45% berdasarkan pre-test dan post-test.

5. Kesimpulan

Penelitian ini mengungkapkan bahwa Penerapan *secure coding* secara konsisten terbukti efektif dalam meningkatkan keamanan aplikasi internal PT. Industri Karet Deli. Penguatan dilakukan melalui kebijakan pengembangan yang lebih ketat, pelatihan developer, dan penerapan sistem review kode. Disarankan agar perusahaan mengintegrasikan *security awareness* ke dalam budaya kerja dan mengadopsi siklus pengembangan perangkat lunak yang aman secara menyeluruh.

REFERENSI

[1] J. Andress, *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice*. Syngress, 2014.
[2] M. Howard and S. Lipner, *The security development lifecycle: A process for developing demonstrably more secure software*. Microsoft Press, 2006.
[3] F. Wadly, Z. Ramadhan, M. Muslim, and D. A. Sitompul, "Design of tidal height monitoring equipment based on the Internet of Things for the preservation of mangroves at Kurnia My Darling Beach," in *Proceeding of International Conference on Artificial Intelligence, Navigation, Engineering, and Aviation Technology (ICANEAT)*, vol. 1, no. 1, pp. 472-476, Nov. 2024.
[4] M. Yusuf, A. Sanny, and Z. Ramadhan, "Deposit strategy of easy wadiah savings fund at Bank Syariah Indonesia," *Lead Journal of Economy and Administration*, vol. 2, no. 3, pp. 125-138, 2024.
[5] Z. Ramadhan and H. Kurniawan, "Use of a mobile-based online public complaint system in Kebun Kelapa Village," *International Journal of Computer Sciences and Mathematics Engineering*, vol. 2, no. 2, pp. 90-99, 2023.
[6] F. Wadly, Z. Ramadhan, and D. A. Sitompul, "Internet of Things based tidal monitoring system at Kurnia My Darling Beach," *Journal of Information Technology, Computer Science and Electrical Engineering*, vol. 1, no. 3, pp. 436-443, 2024.
[7] Z. Ramadhan, F. Wadly, and G. C. Ananda, "E-commerce application design with web-based CodeIgniter framework," *Journal of Information Technology, Computer Science and Electrical Engineering*, vol. 1, no. 3, pp. 96-105, 2024.
[8] [8] Z. Ramadhan and G. C. Ananda, "Implementation of cloud computing database system in education sector for student learning in higher education," *PROSIDING FAKULTAS TEKNIK DAN ILMU KOMPUTER UNIVERSITAS DHARMAWANGSA*, vol. 1, no. 1, pp. 161-169, 2024.
[9] G. McGraw, *Software security: Building security in*. Addison-Wesley, 2006.
[10] OWASP Foundation, "OWASP top ten web application security risks," 2021. [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed: 16-Jun-2025].
[11] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*. International Organization for Standardization, 2013.
[12] D. Kurniawan, *Keamanan jaringan dan sistem informasi*. Deepublish, 2020.
[13] A. Ramadhani and N. Fitriani, "Analisis penerapan secure coding pada aplikasi web berbasis framework Laravel," *Jurnal Teknologi dan Keamanan Informasi*, vol. 9, no. 2, pp. 115-123, 2022.
[14] A. Widodo, *Pengantar keamanan sistem informasi*. Informatika, 2019.
[15] Kaspersky Lab, "What is cybersecurity?" 2023. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Accessed: 16-Jun-2025].
[16] R. A. Budi and D. Santoso, "Evaluasi keamanan aplikasi web menggunakan OWASP ZAP," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 7, no. 1, pp. 89-97, 2021.
[17] OWASP Foundation, "OWASP top ten web application security risks," 2021.
[18] M. Howard and S. Lipner, *The security development lifecycle*. Microsoft Press, 2006.
[19] G. McGraw, *Software security: Building security in*. Addison-Wesley, 2006.
[20] SANS Institute, "Secure coding practices checklist," 2020.
[21] ISO/IEC 27001:2013, *Information security management systems*.