Prosiding Seminar Nasional Sains dan Teknologi Seri III
Fakultas Sains dan Teknologi, Universitas Terbuka
Vol. 2 No. 1 (2025)
e-ISSN: 3047-6569

PENERAPAN DOCKER CONTAINER UNTUK MENDUKUNG MULTI DOMAIN DAN KEAMANAN WEBSITE PEMERINTAH PROVINSI PAPUA

Isnan Wahyudi[1*], Sri Dianing Asri[2*]
[1]Program Studi Sistem Informasi, Universitas Terbuka, Surakarta, Indonesia
[2]Program Studi Teknik Informatika, Universitas Dian Nusantara, Jakarta, Indonesia

**Penulis korespondensi: 043386779@ecampus.ut.ac.id*

ABSTRAK

Kemajuan teknologi informasi telah mendorong pemerintah untuk mengelola website secara aman, efisien, dan fleksibel. Pemerintah Provinsi Papua menghadapi tantangan dalam pengelolaan website multi-domain, terutama terkait keamanan, yang diperburuk oleh insiden akses tidak sah pada awal tahun 2023. Penelitian ini bertujuan untuk menerapkan Docker sebagai platform containerisasi guna meningkatkan keamanan dan efisiensi operasional website multi-domain pemerintah. Metode yang digunakan meliputi analisis kebutuhan infrastruktur, desain arsitektur berbasis container, serta uji coba implementasi pada lingkungan simulasi. Hasil penelitian menunjukkan bahwa penerapan Docker mampu mengisolasi setiap domain dalam container yang terpisah, meminimalkan risiko serangan siber, dan mengoptimalkan sumber daya infrastruktur. Selain itu, pengelolaan multi-domain berbasis Docker terbukti meningkatkan efisiensi deployment dan pemeliharaan sistem secara berkelanjutan. Implikasi dari penelitian ini adalah tersedianya solusi praktis untuk tata kelola website pemerintah yang aman dan andal, sehingga mampu mendukung transparansi informasi dan pelayanan publik yang lebih baik.

Kata kunci: Container, Docker, Keamanan Website, Multi Domain

1. PENDAHULUAN

Pemberlakuan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik pada tanggal 30 April 2010 menjadi momentum penting dalam mendorong keterbukaan informasi di Indonesia, khususnya di Provinsi Papua. Pemerintah daerah, melalui Satuan Kerja Perangkat Daerah (SKPD), diwajibkan untuk menyediakan informasi kepada masyarakat melalui *website* yang dikelola secara profesional. *Website* pemerintah sebagai sarana utama untuk menyampaikan informasi, menyediakan layanan publik dan memastikan transparansi kepada masyarakat. *Website* ini tidak hanya mencerminkan kredibilitas pemerintah, tetapi juga berfungsi sebagai media penghubung yang efektif antara pemerintah dan masyarakat.

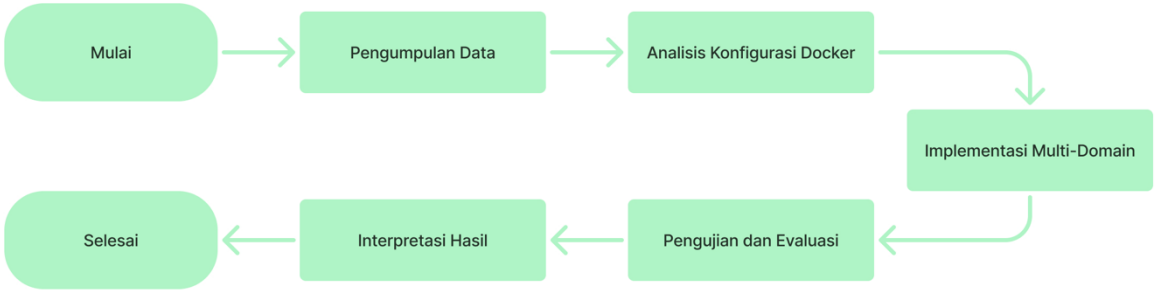
Website pemerintah sering menghadapi berbagai permasalahan, seperti potensi kebocoran data, akses tidak sah, dan serangan siber. Insiden pada awal tahun 2023, di mana domain website SKPD di Provinsi Papua disusupi aplikasi perjudian online, menjadi bukti nyata kelemahan keamanan sistem yang tidak didesain secara memadai. Insiden ini mengakibatkan domain namaskpd.papua.go.id dihentikan sementara (*suspend)*, sehingga mengganggu akses masyarakat terhadap informasi resmi pemerintah. Hal ini menunjukkan perlunya pendekatan baru dalam pengelolaan infrastruktur website pemerintah untuk mengurangi risiko serupa di masa depan.

Teknologi *containerisasi*, seperti Docker, menawarkan solusi praktis untuk mengatasi tantangan tersebut. Docker memungkinkan setiap aplikasi atau domain dijalankan dalam *container* yang terisolasi. Keunggulan Docker dibandingkan metode tradisional seperti *virtual machine* terletak pada efisiensinya dalam penggunaan sumber daya, skalabilitas yang lebih mudah, dan kecepatan proses pengembangan serta *deployment* aplikasi (Dwiyatno et al., 2020; Rivaldi et al., 2020). Teknologi ini juga dapat mendukung pengelolaan multi-domain yang lebih terorganisir dengan menyediakan wadah independen untuk setiap domain, serta memungkinkan penyimpanan data secara terpusat.

Penelitian ini berfokus pada penerapan Docker Container dalam mendukung pengelolaan *website multi-domain* Pemerintah Provinsi Papua. Masalah utama yang diangkat adalah bagaimana Docker dapat membantu meningkatkan keamanan sistem, mendukung efisiensi pengelolaan *multi-domain*, serta mencegah insiden seperti serangan siber. Adapun tujuan penelitian ini adalah untuk mengimplementasikan solusi berbasis Docker guna memperkuat keamanan *website* pemerintah, mendesain arsitektur yang mendukung kebutuhan *multi-domain*, dan memberikan panduan praktis bagi pemerintah dalam mengelola sistem digital secara lebih aman dan efisien.

2. METODE

Penelitian ini menggunakan pendekatan deskriptif dengan metode eksperimental yang bertujuan untuk mengimplementasikan dan mengevaluasi penggunaan Docker dalam mendukung keamanan serta pengelolaan multi-domain *website* Pemerintah Provinsi Papua. Proses penelitian terdiri beberapa tahapan utama yaitu:



Gambar 1. Proses penelitian

a. Pengumpulan Data, proses pengumpulan data melibatkan beberapa langkah, yaitu:
   - Data primer diperoleh melalui observasi langsung terhadap infrastruktur teknologi informasi di lingkungan Pemerintah Provinsi Papua. Observasi ini mencakup analisis perangkat keras, perangkat lunak dan konfigurasi subdomain *website* pada pemerintah Provinsi Papua.
   - Data sekunder dikumpulkan dari berbagai sumber, termasuk dokumen teknis internal, jurnal ilmiah yang relevan, laporan insiden keamanan sebelumnya, serta referensi yang mendukung penerapan Docker Container.

b. Analisis Konfigurasi Docker
   Setelah data terkumpul, dilakukan analisis mendalam terhadap kebutuhan infrastruktur berbasis Docker. Analisis ini meliputi:
   - Evaluasi kemampuan Docker dalam memenuhi kebutuhan, seperti pengelolaan container, isolasi sumber daya dan keamanan aplikasi.

- Peninjauan konfigurasi Docker yang paling sesuai, mencakup pengaturan Docker Compose untuk pengelolaan container.

c. Perancangan Arsitektur Multi-Domain
Desain arsitektur sistem dilakukan berdasarkan hasil analisis sebelumnya. Desain ini mencakup:
- Integrasi komponen tambahan, seperti firewall, mekanisme load balancing, serta sistem logging dan monitoring untuk mendukung operasional yang aman dan efisien.
- Penyusunan rencana implementasi, mencakup alur kerja otomatis (CI/CD) untuk penerapan pembaruan sistem secara berkala.

d. Implementasi Multi-Domain
Tahapan implementasi dilakukan dengan mengonfigurasi Docker sesuai rancangan arsitektur. Beberapa langkah utama meliputi:
- Pembuatan container terpisah untuk setiap domain yang dikelola.
- Pengaturan Docker Compose untuk mengelola dependensi antar container, termasuk integrasi dengan database terpusat.
- Pengujian awal sistem untuk memastikan konfigurasi berjalan tanpa kendala.

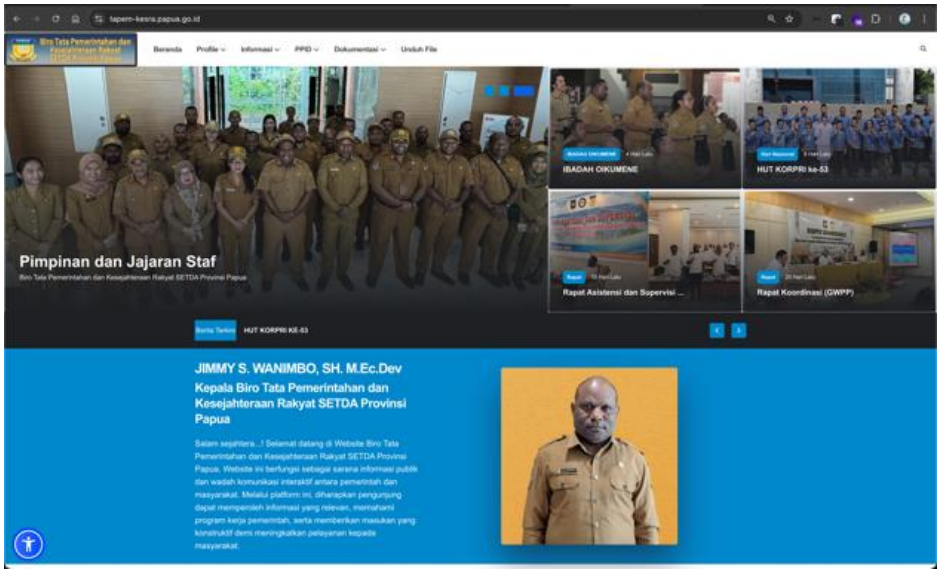
e. Pengujian dan Evaluasi
Pada tahap ini, dilakukan pengujian sistem untuk mengevaluasi kinerja dan keamanan arsitektur yang telah diimplementasikan. Pengujian mencakup:
- Simulasi serangan siber seperti SQL injection, brute force, dan DDoS untuk mengukur efektivitas keamanan sistem.
- Uji beban untuk mengukur efisiensi dalam pengelolaan multi-domain, termasuk waktu respons server dan tingkat penggunaan sumber daya.
- Evaluasi pengalaman pengguna berdasarkan wawancara dengan administrator sistem dan pengguna akhir.

f. Interpretasi Hasil, hasil pengujian dianalisis secara kuantitatif dan kualitatif:
- Data kuantitatif meliputi penggunaan CPU dan memori, waktu respons, serta tingkat keberhasilan mitigasi serangan siber.
- Data kualitatif diinterpretasikan dari wawancara dan evaluasi pengalaman pengguna terkait pengelolaan dan keandalan sistem.

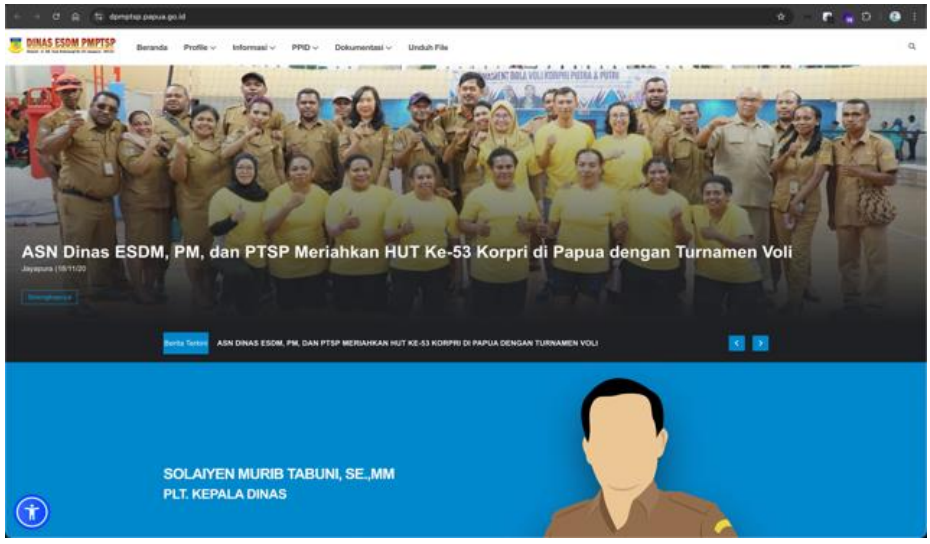
3. HASIL DAN PEMBAHASAN

3.1 Hasil

Penelitian ini menghasilkan beberapa temuan utama terkait penerapan *Docker Container* untuk mendukung keamanan dan pengelolaan *multi-domain* pada *website* Pemerintah Provinsi Papua. Berikut ini contoh dari hasil *website* multi-domain pada Pemerintahan Provinsi Papua



Gambar 2. Website tapem-kesra.papua.go.id



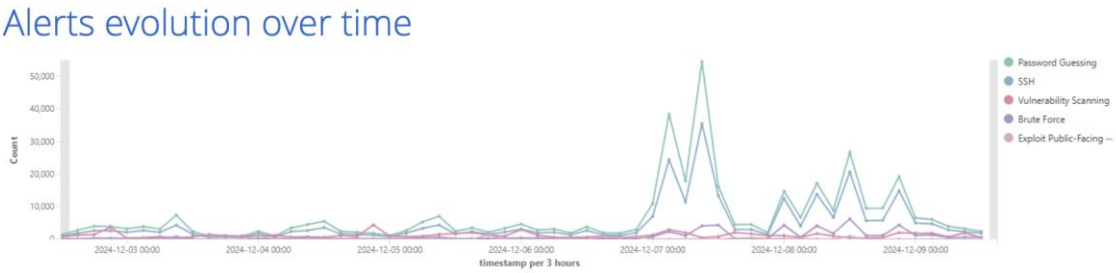
Gambar 3. Website dpmptsp.papua.g.id

3.1.1 Peningkatan Keamanan *Website*

Implementasi Docker mampu meningkatkan isolasi aplikasi melalui penggunaan container. Setiap container bertindak sebagai lingkungan yang terisolasi, sehingga serangan pada satu domain tidak berdampak pada domain lain.

Berdasarkan Generating Report yang diperoleh dari pihak Kominfo Provinsi Papua selaku tim yang bertugas disisi server, diperoleh grafik hasil pengujian menggunakan *Wazuh Module Agents*. Grafik ini memberikan gambaran mengenai aktivitas serangan yang terdeteksi, seperti *Password Guessing*, *SSH*, *Vulnerability Scanning*, *Brute Force*, dan *Exploit Public-Facing*. Berikut ini *Generating Report* grafik hasil pengujian dengan *wazuh module agents*:

a. *Alerts Evolution Over Time*

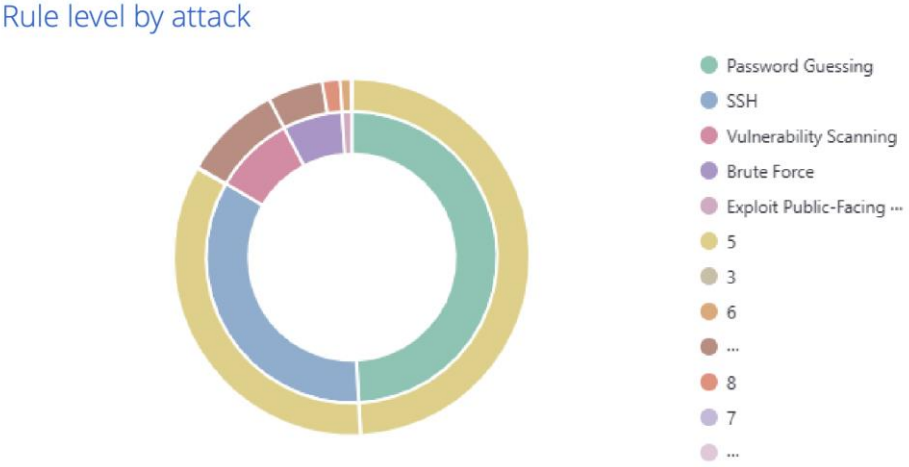


Gambar 4. *Report Alerts Evolution Over Time*

Grafik ini menunjukkan perkembangan jumlah peringatan dari waktu ke waktu, memberikan gambaran tentang tren serangan yang mungkin terjadi. Misal yang terlihat dari grafik diatas terdapat aktifitas pada tanggal 03 Desember 2024 sampai dengan 09 Desember 2024:

- *Password Guessing* yaitu upaya penyerang untuk menebak kata sandi pengguna dengan mencoba berbagai kombinasi, serangan ini mencapai angka sekitar 50.000.
- *SSH (Secure Shell)* yaitu protokol yang digunakan untuk mengakses perangkat secara aman. Serangan terhadap *SSH* sering kali melibatkan upaya untuk mendapatkan akses tidak sah melalui autentikasi yang gagal, serangan ini mencapai angka sekitar 32.000.
- *Vulnerability Scanning* yaitu proses pemindaian sistem oleh penyerang untuk menemukan kerentanan yang dapat dieksploitasi, serangan ini mencapai angka sekitar 3.000.
- *Brute Force* yaitu metode di mana penyerang mencoba semua kemungkinan kombinasi untuk mendapatkan akses ke akun atau system, serangan ini mencapai angka sekitar 2.000.
- *Exploit Public-Facing* yaitu Serangan ini menargetkan aplikasi atau layanan yang dapat diakses publik untuk mengeksploitasi kerentanan yang ada, serangan ini mencapai angka sekitar 900.

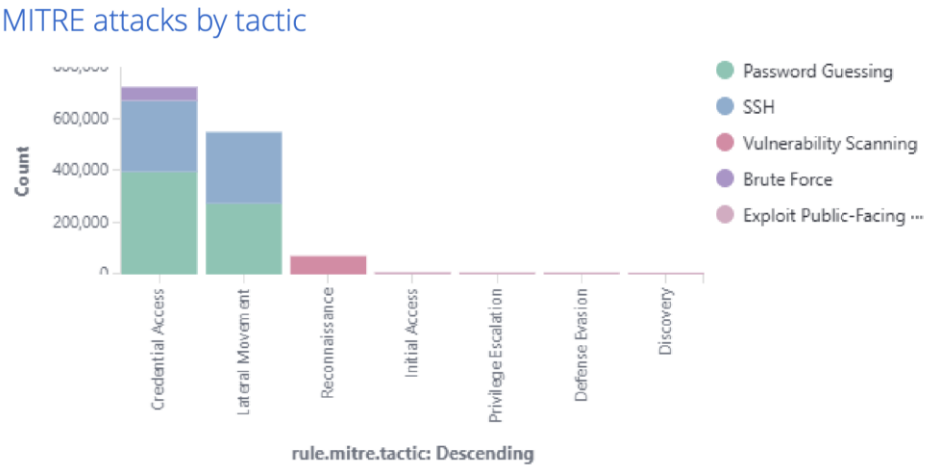
b. *Rule Level by Attack*



Gambar 5. *Report Rule Level by Attack*

Grafik ini menunjukkan tingkat keparahan (level) dari berbagai aturan yang diterapkan pada serangan tertentu. Setiap serangan yang terdeteksi akan memiliki level yang berbeda, yang mencerminkan seberapa serius ancaman. Level ini biasanya berkisar dari 1 hingga 10, di mana angka yang lebih tinggi menunjukkan tingkat keparahan yang lebih besar.

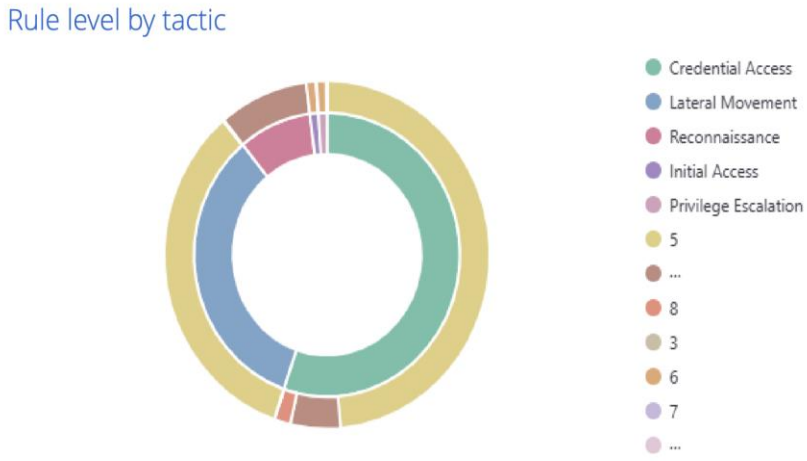
c. *MITRE Attacks by Tactic*



Gambar 6. *Report MITRE Attacks by Tactic*

Mengelompokkan serangan berdasarkan taktik yang digunakan, memberikan gambaran tentang jenis serangan yang paling sering terjadi dan bagaimana mereka terkait dengan taktik tertentu dalam kerangka *MITRE ATTACK*. Berfungsi untuk memahami konteks serangan dan mengidentifikasi area yang perlu diperkuat dalam pertahanan keamanan.

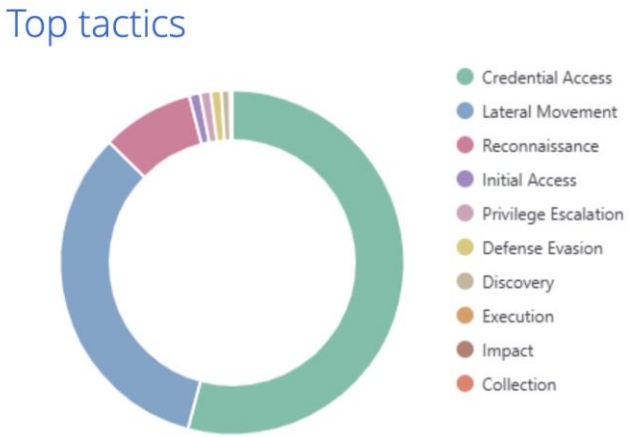
d. *Rule Level by Tactic*



Gambar 7. *Report Rule Level by Tactic*

Grafik ini mengelompokkan serangan berdasarkan taktik yang digunakan, dan menunjukkan tingkat keparahan dari aturan yang diterapkan untuk masing-masing taktik. Dengan memahami taktik yang digunakan dan tingkat keparahan yang terkait, organisasi dapat lebih baik memfokuskan upaya pertahanan mereka pada area yang paling rentan dan berisiko tinggi.

e. *Top Tactics*



Gambar 8. *Report Top Tactics*

Grafik ini merangkum taktik-taktik utama yang digunakan oleh penyerang berdasarkan data yang dikumpulkan. Memberikan wawasan tentang metode yang paling umum digunakan dalam serangan, yang dapat membantu dalam merencanakan langkah-langkah mitigasi.

f. *Table Alerts Summary*

Mencantumkan ID, deskripsi peringatan, level keparahan, dan jumlah kejadian untuk beberapa jenis peringatan yang terdeteksi. Contohnya, peringatan dengan ID 5760 menunjukkan bahwa ada 165.392 kali kegagalan autentikasi yang menunjukkan potensi serangan brute force atau upaya akses tidak sah.

Alerts summary

Rule ID	Description	Level	Count
5760	sshd: authentication failed.	5	165392
5503	PAM: User login failed.	5	121447
5710	sshd: Attempt to login using a non-existent user	5	108391
31151	Multiple web server 400 error codes from same source ip.	10	71713
2502	syslog: User missed the password more than one time	10	21924
5758	Maximum authentication attempts exceeded.	8	12903
5551	PAM: Multiple failed logins in a small period of time.	10	12089
31104	Common web attack.	6	6054
40111	Multiple authentication failures.	10	2851
5763	sshd: brute force trying to get access to the system. Authentication failed.	10	2637
31164	SQL injection attempt.	6	1135
31105	XSS (Cross Site Scripting) attempt.	6	934
5706	sshd: insecure connection attempt (scan).	6	772
5712	sshd: brute force trying to get access to the system. Non existent user.	10	730
31106	A web attack returned code 200 (success).	6	605
31153	Multiple common web attacks from same source ip.	10	593
31533	High amount of POST requests in a small period of time (likely bot).	10	491
31103	SQL injection attempt.	7	467
31509	CMS (WordPress or Joomla) login attempt.	3	463
31516	Suspicious URL access.	6	355
3398	Postfix: Illegal address from unknown sender	6	173
31110	PHP CGI-bin vulnerability attempt.	6	95
31168	Shellshock attack detected	15	76
5701	sshd: Possible attack on the ssh server (or version gathering).	8	56
31152	Multiple SQL injection attempts from same source ip.	10	48
31515	PHPMyAdmin scans (looking for setup.php).	6	38
31154	Multiple XSS (Cross Site Scripting) attempts from same source ip.	10	36
31166	Shellshock attack attempt	6	22
550	Integrity checksum changed.	7	15
31115	URL too long. Higher than allowed on most browsers. Possible attack.	13	4
5501	PAM: Login session opened.	3	4
5715	sshd: authentication success.	3	2

Gambar 9. *Table Alerts Summary*

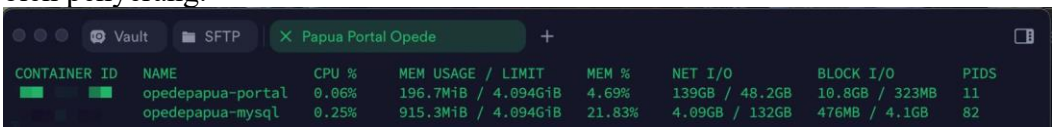
3.1.2 Efisiensi Pengelolaan Multi-Domain

Dengan desain arsitektur berbasis Docker, multi-domain *website* dapat dikelola lebih efisien. Satu kode induk dapat digunakan untuk beberapa domain melalui mekanisme containerisasi, sementara data disimpan terpusat dalam satu wadah database. Pengujian efisiensi menunjukkan penghematan waktu *deployment* hingga 40% dibandingkan metode tradisional. Multi-domain pada *website* SKPD Pemerintah Papua terdapat 23 sub-domain dan waktu *deployment* sekitar dua bulan.

Gambar 10. Multi-domain webiste SKPD Provinsi Papua

3.1.3 Pengurangan Risiko Insiden Keamanan

Implementasi Docker untuk mendukung multi-domain *website* Pemerintah Provinsi Papua memastikan bahwa setiap layanan subdomain berjalan dalam lingkungan terkontrol dan terstandarisasi melalui containerisasi. Dengan menggunakan satu kode induk untuk semua subdomain, supaya dapat mencegah risiko serangan. Stabilitas system terjamin dengan optimalisasi sumber daya server, sehingga mengurangi risiko *overload* yang dapat dieksploitasi oleh penyerang.



Gambar 11. Docker Status

Hasil pemantauan dengan perintah *docker stats* menunjukkan bahwa container opedepapua-portal memiliki trafik jaringan tinggi (139GB RX) dengan penggunaan memori rendah (4.69%), menandakan layanan portal berjalan efisien tanpa membebani server. Sementara itu, container opedepapua-mysql menggunakan lebih banyak memori (21.83%) dan memiliki aktivitas I/O disk signifikan (4.1GB *write*), yang wajar untuk sistem database yang menangani banyak permintaan baca/tulis. Hal ini menunjukkan stabilitas sistem yang lebih terkontrol, mencegah risiko *overload*, serta mendukung mitigasi kerentanan keamanan melalui lingkungan terstandarisasi yang lebih mudah dikelola.

3.2 Pembahasan

3.2.1 Implementasi Docker untuk Keamanan *Website*

Salah satu keunggulan utama Docker adalah kemampuan untuk mengisolasi aplikasi dalam container terpisah. Berdasarkan penelitian Dwiyatno et al. (2020), isolasi ini mampu mencegah serangan yang memanfaatkan kerentanan sistem utama. Pada penelitian ini, isolasi container meminimalkan dampak serangan, sehingga meningkatkan keandalan sistem *website* pemerintah. Berikut ini konfigurasi *code docker-compose.yml* pada *deploy localhost*:

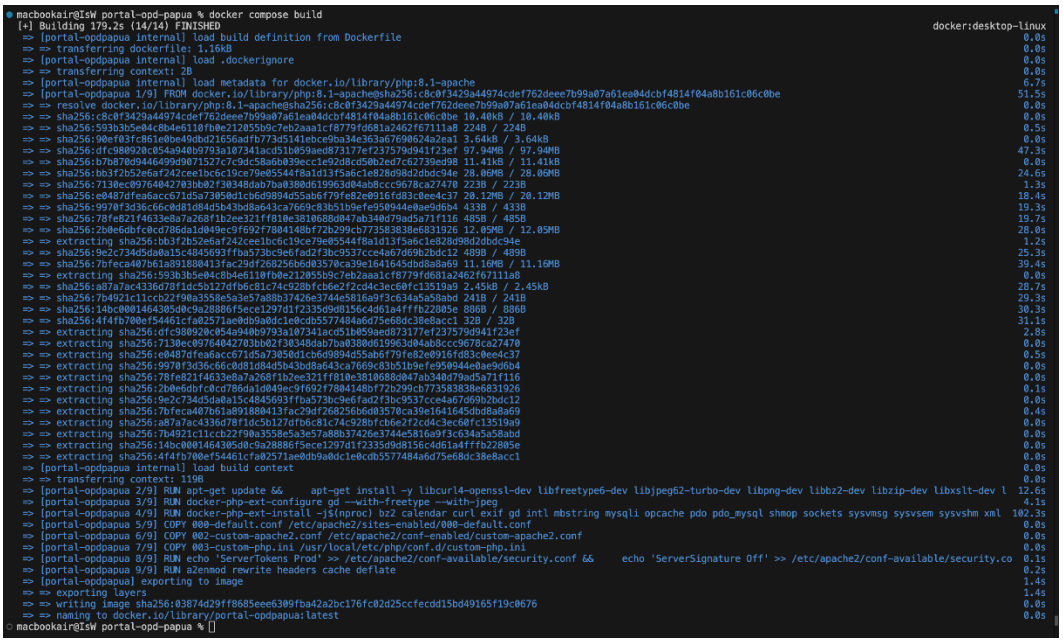
```
X-compose-project:
  project_name: web-opede-papua
services:
  portal-opdpapua:
    container_name: portal-opdpapua
    hostname: portal-opdpapua
    image: portal-opdpapua:latest
    restart: unless-stopped
    ports:
      - "${WEB_PORT}:80"
    environment:
      - TZ=Asia/Jayapura
    volumes:
      - ./portal:/var/www/html
      - ./log/:/var/log
    build:
      context: ./build
      dockerfile: Dockerfile
    depends_on:
      - opedepapua-mysql
    networks:
      - portal-opdpapua-network

  opedepapua-mysql:
    container_name: opedepapua-mysql
    hostname: opedepapua-mysql
    image: mysql:8
    restart: unless-stopped
    ports:
      - "127.0.0.1:${DB_PORT}:3306"
    environment:
      - TZ=Asia/Jayapura
      - MYSQL_ROOT_PASSWORD=${DB_PASSWORD}
    volumes:
      - ./mysql:/var/lib/mysql
    networks:
      - portal-opdpapua-network

networks:
  portal-opdpapua-network :
    driver: bridge
    name: portal-opdpapua-network
```

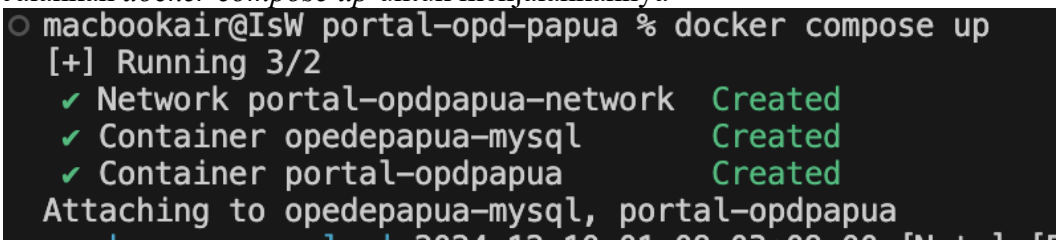
Gambar 12. *konfigurasi code docker-compose.yml* pada *deploy localhost*

Dan saat di *docker compose build*:



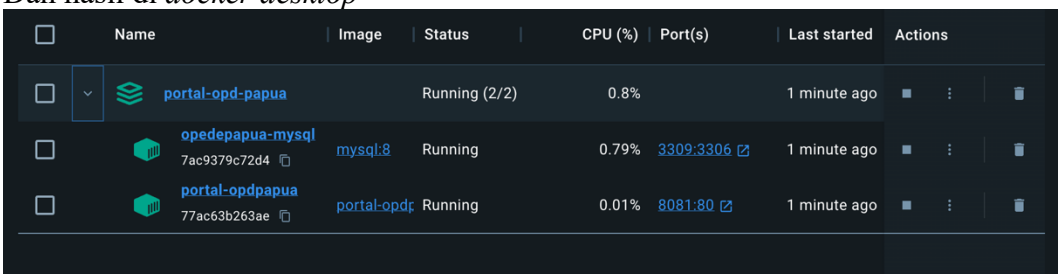
Gambar 13. docker compose

Jalankan *docker compose up* untuk menjalankannya



Gambar 14. docker compose up

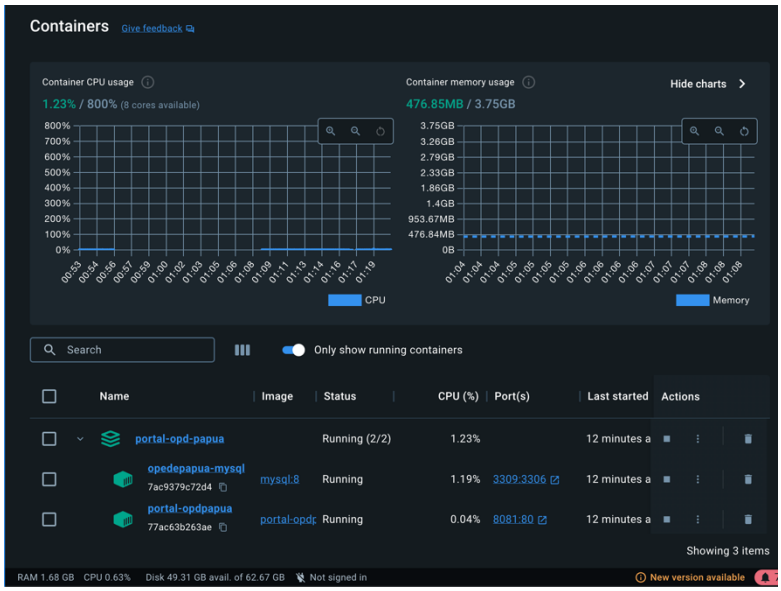
Dan hasil di *docker desktop*



Gambar 15. *Docker destop*

3.2.2 Dukungan *Docker* pada Arsitektur *Multi-Domain*

Pengelolaan *multi-domain* berbasis *Docker* memungkinkan penggunaan sumber daya yang lebih optimal. Temuan ini konsisten dengan studi Rivaldi et al. (2020), yang menunjukkan bahwa penggunaan *Docker Swarm* dapat meningkatkan ketersediaan dan efisiensi sistem *multi-domain*. Hasil implementasi pada penelitian ini menunjukkan bahwa pendekatan *containerisasi* mempermudah pengelolaan domain yang kompleks, tanpa mengorbankan performa.

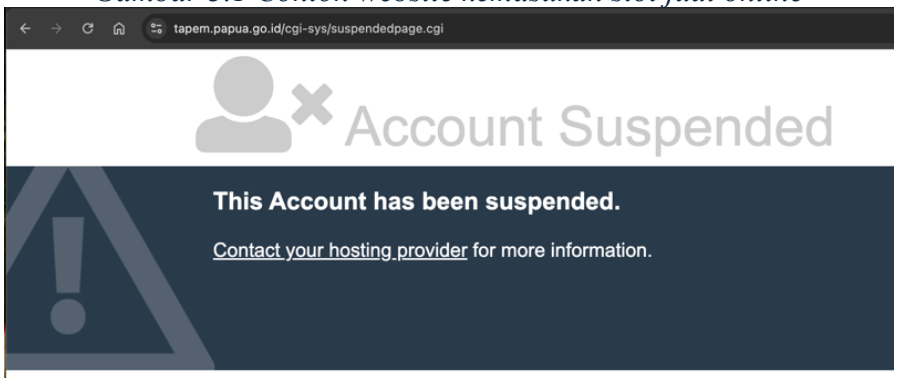


Gambar 16. Performa Docker pada multi-domain website Pemerintahan Papua

3.2.3 Mitigasi Risiko Keamanan melalui *Docker*

Penggunaan *Docker* untuk membangun sistem yang lebih aman diperkuat oleh penambahan lapisan keamanan seperti pengaturan *firewall* dan *reverse proxy*. Studi oleh Khalida et al. (2019) juga menekankan pentingnya mengintegrasikan *Docker* dengan sistem keamanan tambahan untuk memitigasi risiko akses tidak sah. Implementasi dalam penelitian ini berhasil menurunkan risiko serangan siber secara signifikan, yang sebelumnya menyebabkan *suspend* pada domain namaskpd.papua.go.id.

Gambar 3.1 Contoh website kemasukan slot judi online



Gambar 17. Contoh website terkena suspend

4. KESIMPULAN

Penelitian ini menemukan bahwa penerapan Docker Container secara signifikan meningkatkan keamanan dan efisiensi pengelolaan multi-domain pada *website* Pemerintah Provinsi Papua. Teknologi containerisasi mendukung pencapaian tujuan penelitian yaitu menciptakan lingkungan pengelolaan *website* yang aman, efisien dan andal. Penggunaan satu master *code* untuk semua subdomain memungkinkan pengelolaan multi-domain yang lebih terstruktur, mengurangi konflik antar system dan mempercepat proses *deployment*. Hasil pengujian menunjukkan bahwa Docker dapat mengoptimalkan sumber daya server, mendukung stabilitas layanan dan mengurangi risiko *overload* yang dapat dimanfaatkan oleh penyerang. Relevansi penelitian ini terletak pada kontribusinya dalam mendukung transformasi digital pemerintah daerah melalui teknologi modern yang mampu menjaga keandalan dan keamanan layanan publik berbasis digital. Dengan hasil ini, penelitian memberikan landasan teknis untuk implementasi containerisasi di sektor publik sebagai solusi efektif menghadapi tantangan digitalisasi.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada dosen pembimbing atas bimbingan yang berharga selama proses penelitian ini. Ucapan terima kasih juga disampaikan kepada tim Kominfo yang telah memberikan kepercayaan dalam mengerjakan proyek ini, serta pimpinan perusahaan yang telah memberikan kesempatan dan dukungan penuh dalam pelaksanaannya. Penghargaan setinggi-tingginya juga diberikan kepada tim kerja yang telah bekerja sama dengan dedikasi tinggi dalam menyelesaikan proyek ini. Tak lupa, terima kasih kepada pihak-pihak lain yang tidak dapat disebutkan satu per satu atas dukungan dan kontribusi yang telah diberikan hingga penelitian ini dapat terselesaikan dengan baik.

DAFTAR PUSTAKA

Dwiyatno S, Rakhmat E, Gustiawan O. (2020). Implementasi Virtualisasi Server Berbasis Docker Container, 7(2), 165–175.

Fadlulloh M, Bik R. (2017). Implementasi Docker Untuk Pengelolaan Banyak Aplikasi Web. Jurnal Sistem Informasi dan Teknologi, 7(2), 46–50.

Rivaldi A, Darusalam U, Hidayatullah D. (2020). Perancangan Multi Node Web Server Menggunakan Docker Swarm dengan Metode Highavability, 4(3), 529–534.

Setyoko, Zahra (2024). Perbandingan Efisiensi Proses CI/CD Multi-Lingkungan melalui Implementasi Paralel dan Berurutan. Jurnal Rekayasa Perangkat Lunak, 4(3), 911–925.

Rakhmi Khalida, Adi Muhajirin, Siti Setiawati (2019). Teknis Kerja Docker Container untuk Optimalisasi Penyebaran Aplikasi. Jurnal Teknologi Komputer dan Informasi, 7(2), 167-176.

Asmara R, Fajri A, Novina. (2024). Membangun Pengelolaan Aplikasi Web Berbasis Docker pada Kominfo Padang Panjang, 4(1), 17-21.

Dame A, Zailani A. (2023). Implementasi Webserver Berbasis Docker Dan Linux, 1(5), 1084-1090.

Isron, Muhammad Hussein. (2021). Implementasi Virtual Server Berbasis Container Pada Sistem Informasi Geografis Cagar Budaya Mojokerto, 1(5), 2686-2220.

Alamsyah, Wahanani (2021). Penerapan Docker Untuk Membangun Infrastruktur Private Cloud Storage Berbasis Iaas, 2(2), 122-131

Ariadi F, Iswahyudi C (2022). Penerapan Docker Container Sebagai Teknologi Ramah Skalabilitas Dibanding Teknik Virtualisasi Untuk Membangun Website Di Ubuntu 18.04.4 Lts, 8(2), 47-57.

Al Amien J, Winarso D (2019). Analisis Peningkatan Kinerja Ftp Server Menggunakan Load Balancing Pada Container, 9(3), 8-18.

Teteki, A., Muryanto, B., dan Adikara, G. (2023). *Handbook Digital Safety*. Yogyakarta: Yayasan LKiS.

Asrin, F., Ismarmiaty, I., Putra, S. A. S., Setyoningrum, N. G., Yuliana, A., Juwari, T. E., Harsapranata, A. I., Saleh, A., Fitri, N. A., Alia, P. A., Ekawati, N., Nofarita, E., dan Setiawan, I. (2024). *Keamanan Sistem Informasi*. Yogyakarta: PT Penamuda Media.

Raharjo, B. (2021). *Keamanan Sistem Informasi*. Semarang: Yayasan Primaagus Teknik.

Yusnita Sari, Ika, Muttaqin, Jamaludin, Simarmata, Janner, Rahman, M. Arif, Iskandar, Akbar, Pakpahan, Andrew Fernando, Karim, Abdul, Sugianto, Yo Ceng Giap, Hazriani, Devi Yendrianof, Manullang, Sardjana Orba. (2020). *Keamanan Data dan Informasi*. Medan: Yayasan Kita Menulis.

Fauzi, Ahmad, Setiawan, Ade, Bayu Hasta, Andika, Maulana, Andry, Permana, Rifky. (2022). *Introduction Cyber Security*. Bengkulu: Elite Media Kreazi.

Hanafi. (2022). *Dasar Cyber Security dan Forensic*. Yogyakarta: Deepublish Publisher.