BAB 4
HASIL PENELITIAN

4.1 Ringkasan Hasil Penelitian

Penelitian ini berhasil mengimplementasikan sistem pemantauan keamanan jaringan berbasis honeypot OpenCanary yang terintegrasi dengan ELK Stack (Elasticsearch, Logstash, Kibana) sebagai upaya deteksi dini terhadap serangan siber di lingkungan Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA). Sistem dibangun dan diuji pada jaringan laboratorium menggunakan perangkat fisik dan VPS, kemudian diimplementasikan ke jaringan publik setelah integrasi dinyatakan stabil dan fungsional.

Sistem honeypot OpenCanary dikonfigurasi untuk mensimulasikan layanan umum seperti FTP, HTTP, SSH, SMTP, Telnet, MySQL, SMB, RDP, MSSQL, Git, serta menghasilkan log dalam format JSON yang dikirim secara *real-time* ke sistem ELK Stack melalui Filebeat. Data log yang masuk diproses oleh Logstash, diindeks oleh Elasticsearch, dan divisualisasikan melalui Kibana dalam bentuk dashboard interaktif.

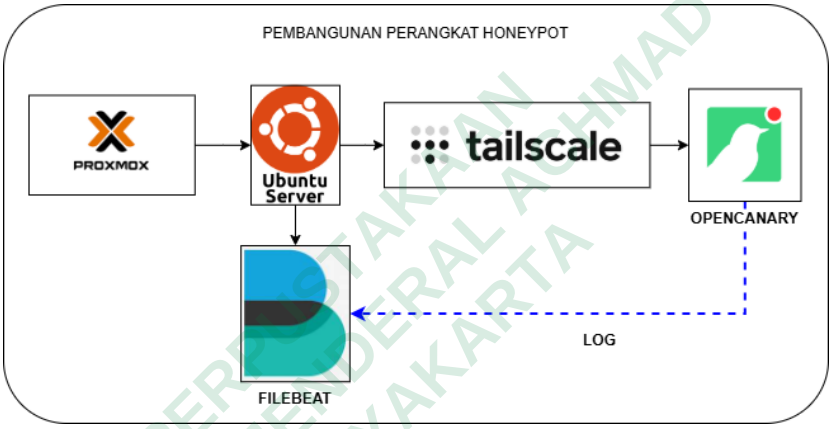
Selama periode monitoring selama 30 hari, sistem mencatat total sebanyak 2.209.032 entri log aktivitas dengan rata-rata 73.634 log per hari. Data yang dikumpulkan menunjukkan berbagai pola serangan yang bersifat otomatis dan tersebar sepanjang hari. Port yang paling sering diserang adalah 3389 (RDP)**,** 1433 (SQL Server)**,** dan 22 (SSH)**.** Sementara itu, negara asal serangan terbanyak adalah Vietnam, Tiongkok, dan Indonesia, dengan IP tertentu muncul secara konsisten dan berulang, mengindikasikan penggunaan botnet atau skrip otomatis.

Visualisasi dalam Kibana berhasil menampilkan data serangan secara real-time dalam berbagai bentuk grafik dan tabel, termasuk tren serangan, IP sumber serangan terbanyak, distribusi port tujuan, kategori aktivitas (logtype), hingga peta geografis asal negara penyerang. Selain itu, penyesuaian sistem juga dilakukan pada tahap implementasi, termasuk penambahan *GeoIP* untuk memperkaya data, serta peningkatan spesifikasi server agar performa sistem tetap optimal.

4.2 Implementasi Sistem

4.2.1 Pembangunan Perangkat Honeypot

Pembangunan perangkat OpenCanary dilakukan secara bertahap, dimulai dari penyediaan infrastruktur virtual menggunakan *Proxmox Virtual Environment* (Proxmox VE), instalasi sistem operasi Ubuntu Server 22.04 LTS sebagai dasar sistem, hingga pemasangan dan pengujian honeypot OpenCanary sebagai komponen utama untuk menangkap aktivitas mencurigakan di jaringan. Proses ini bertujuan untuk memastikan bahwa perangkat OpenCanary berjalan stabil dan dapat berfungsi sebagaimana mestinya.



Gambar 4.1 Pembangunan Perangkat Honeypot OpenCanary

A. Proxmox Virtual Environment

Proxmox Virtual Environment (Proxmox VE) dipilih sebagai platform virtualisasi dalam penelitian ini karena bersifat *open-source*, ringan, dan mendukung pembuatan serta pengelolaan mesin virtual (VM) secara fleksibel. Proxmox VE diinstal langsung pada server fisik sebagai bare-metal hypervisor**,** sehingga mampu memberikan kinerja virtualisasi yang optimal tanpa bergantung pada sistem operasi tambahan.

Tahap persiapan dilakukan dengan mengunduh berkas instalasi Proxmox VE dalam format ISO dari situs resmi, kemudian membuat media instalasi bootable menggunakan perangkat lunak khusus. Perangkat keras yang digunakan telah mendukung fitur virtualisasi, yang diaktifkan melalui pengaturan BIOS. Langkah ini bertujuan untuk memastikan bahwa proses

instalasi berjalan lancar dan sistem mampu menjalankan mesin virtual dengan stabil.

Proses instalasi dimulai dengan mem-boot sistem dari media instalasi yang telah disiapkan. Pengguna diarahkan untuk memilih opsi instalasi Proxmox VE dan mengikuti sejumlah konfigurasi awal, seperti persetujuan lisensi, pemilihan media penyimpanan, pengaturan zona waktu, negara, serta tata letak papan ketik. Selain itu, pengguna menetapkan kata sandi administrator dan alamat email sebagai informasi kontak sistem. Pada akhir tahap instalasi, dilakukan konfigurasi jaringan dengan menetapkan alamat IP statik dan parameter jaringan lainnya untuk memastikan konektivitas yang konsisten.

Setelah instalasi selesai dan sistem berhasil melakukan booting, pengguna dapat mengakses antarmuka web Proxmox VE melalui peramban dengan mengetikkan alamat IP yang telah ditetapkan, menggunakan protokol HTTPS dan port 8006. Antarmuka berbasis web ini menyediakan kemudahan dalam pengelolaan infrastruktur virtualisasi, seperti pembuatan dan pengaturan mesin virtual, pemantauan sumber daya, serta manajemen jaringan virtual. Fitur-fitur ini sangat mendukung kebutuhan sistem eksperimental dalam penelitian, sekaligus mempermudah proses pengembangan dan pemantauan sistem secara terpusat.

B. Implementasi Ubuntu Server Pada Proxmox VE

Ubuntu Server 22.04 LTS dipilih sebagai sistem operasi utama pada mesin virtual dalam lingkungan virtualisasi Proxmox VE karena menyediakan dukungan jangka panjang (*Long Term Support*) selama lima tahun, yang sangat relevan dengan kebutuhan sistem penelitian yang mengutamakan stabilitas, keamanan, dan keandalan jangka panjang. Sistem operasi ini juga dikenal ringan dan efisien, serta mendukung berbagai perangkat lunak seperti honeypot OpenCanary dan ELK Stack untuk pemantauan log. Keunggulan lainnya mencakup dokumentasi teknis yang luas, komunitas pengguna yang aktif, dan fleksibilitas tinggi dalam

konfigurasi jaringan dan terminal, menjadikannya solusi ideal untuk implementasi dalam infrastruktur virtual yang dibangun.

Proses implementasi diawali dengan mempersiapkan berkas instalasi Ubuntu Server dalam format ISO yang diunduh langsung dari situs resmi untuk menjamin keaslian perangkat lunak. Berkas ini kemudian diunggah ke lingkungan Proxmox melalui antarmuka web, dan disimpan pada penyimpanan internal sistem virtualisasi untuk digunakan sebagai media instalasi saat pembuatan mesin virtual.

Pembuatan mesin virtual dilakukan melalui fitur yang tersedia di Proxmox VE, dengan menetapkan nama mesin virtual, node fisik yang digunakan, serta memilih berkas ISO Ubuntu Server sebagai sistem operasi. Konfigurasi sistem mencakup penyesuaian jenis BIOS, alokasi sumber daya seperti CPU, RAM, dan kapasitas penyimpanan. Pada tahap pengaturan jaringan, mesin virtual dikonfigurasi menggunakan mode jembatan (*bridged mode)*, sehingga mesin virtual dapat berinteraksi langsung dengan jaringan fisik, memperoleh alamat IP dari jaringan yang sama, dan berfungsi seolah-olah sebagai perangkat independen dalam topologi jaringan.

Instalasi Ubuntu Server pada mesin virtual dilanjutkan dengan pengaturan awal seperti pemilihan bahasa, konfigurasi jaringan (otomatis melalui DHCP atau secara manual dengan IP statik), penetapan nama sistem, serta pembuatan akun pengguna utama. Proses instalasi dilakukan secara otomatis hingga selesai, dan diakhiri dengan proses pemuatan ulang (*reboot*) sistem untuk memastikan konfigurasi telah diterapkan dengan baik. Mesin virtual yang telah dikonfigurasi kemudian siap digunakan sebagai komponen utama dalam sistem pemantauan keamanan jaringan yang dikembangkan.

C. Tailscale

Dalam proses implementasi dan pemantauan honeypot OpenCanary secara jarak jauh, *Tailscale* diadopsi sebagai solusi *Virtual Private Network* (VPN) berbasis protokol *WireGuard*. *Tailscale* memungkinkan terbentuknya konektivitas yang aman antara perangkat yang berada di

jaringan berbeda, tanpa memerlukan konfigurasi yang kompleks seperti *port forwarding* atau penyesuaian *firewall* jaringan internal. Hal ini menjadi solusi praktis dan efisien dalam konteks pemantauan dari luar jaringan kampus.

Instalasi *Tailscale* dilakukan pada *server* honeypot OpenCanary berbasis *Ubuntu Server* dengan langkah-langkah yang mencakup pembaruan sistem untuk memastikan seluruh paket dalam kondisi terbaru, serta pemasangan perangkat lunak *Tailscale* melalui metode yang disediakan secara resmi oleh pengembang. Setelah berhasil diinstal, proses aktivasi dilakukan dengan menghubungkan *server* ke akun *Tailscale* melalui mekanisme otentikasi berbasis browser. Setelah otentikasi selesai, server secara otomatis tergabung dalam jaringan privat *Tailscale* dan memperoleh alamat IP internal yang dapat digunakan untuk mengaksesnya dari jarak jauh.

Dengan implementasi ini, dapat dilakukan pemantauan dan pengelolaan sistem honeypot melalui koneksi terenkripsi dan aman menggunakan protokol SSH. Konfigurasi ini tidak hanya menyederhanakan proses integrasi antar jaringan, tetapi juga mendukung keberlangsungan pemantauan sistem keamanan secara *real-time* dari luar lingkungan kampus tanpa mengorbankan aspek keamanan jaringan

D. OpenCanary

Pemilihan OpenCanary sebagai komponen utama dalam sistem honeypot didasarkan pada kemampuannya dalam mensimulasikan berbagai layanan jaringan yang umum dijadikan sebagai titik masuk serangan, seperti SSH, HTTP, FTP, dan protokol lainnya. Aplikasi ini memiliki keunggulan dalam hal ringan, fleksibel, dan mudah dikonfigurasi, sehingga cocok digunakan dalam lingkungan penelitian maupun produksi, khususnya pada sistem dengan sumber daya terbatas. Selain itu, OpenCanary mendukung integrasi dengan sistem pemantauan log seperti ELK Stack, yang memungkinkan pencatatan dan visualisasi data serangan secara *real-time.*

Proses implementasi OpenCanary dimulai dengan mempersiapkan lingkungan sistem operasi Ubuntu Server yang telah diperbarui. Selanjutnya dilakukan pemasangan dependensi seperti *Python* dan *virtual environment* untuk menjamin instalasi dapat berjalan secara terisolasi dan terstruktur. Setelah itu, OpenCanary diinstal ke dalam lingkungan virtual yang telah dibuat, memungkinkan pemisahan dari sistem utama dan mempermudah pengelolaan komponen.

Tahap berikutnya adalah konfigurasi, di mana OpenCanary disesuaikan untuk mensimulasikan layanan tertentu yang rawan diserang, seperti FTP, HTTP, dan SSH. Konfigurasi dilakukan melalui berkas pengaturan yang memuat parameter seperti port layanan, banner, dan versi layanan palsu. Selain itu, sistem juga dikonfigurasi agar log aktivitas yang dihasilkan dapat dipantau oleh *Filebeat* dan diteruskan ke sistem ELK Stack, guna mendukung proses monitoring secara terintegrasi.

Setelah konfigurasi selesai, OpenCanary dijalankan sebagai layanan aktif yang siap memantau dan mencatat setiap aktivitas mencurigakan terhadap layanan-layanan yang disimulasikan. Sistem ini kemudian secara otomatis mencatat interaksi dari alamat IP penyerang ke dalam berkas log yang dapat dianalisis lebih lanjut. Dengan implementasi ini, OpenCanary berperan sebagai komponen kunci dalam deteksi dini terhadap ancaman siber di lingkungan jaringan UNJAYA.

E. Filebeat

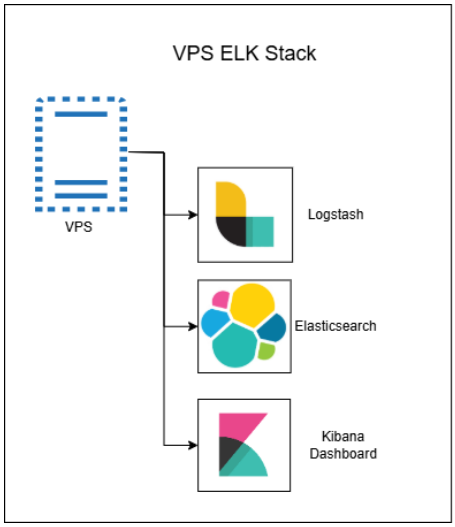
Tahap akhir dari proses implementasi honeypot OpenCanary adalah pengintegrasian *Filebeat* sebagai agen pengiriman log ke dalam sistem pemantauan berbasis ELK Stack. *Filebeat* berfungsi sebagai komponen yang mengambil log aktivitas yang dihasilkan oleh OpenCanary, lalu mengirimkannya ke Logstash untuk diproses dan dianalisis lebih lanjut. Dengan menggunakan *Filebeat*, proses pengiriman log menjadi lebih efisien dan *real-time*, sehingga mendukung visibilitas sistem terhadap potensi ancaman siber.

Proses implementasi diawali dengan pemasangan *Filebeat* pada sistem *Ubuntu Server* yang menjalankan OpenCanary. Setelah terpasang, F*ilebeat* dikonfigurasi untuk membaca file log dari direktori tertentu, yakni file log yang dihasilkan oleh OpenCanary. Selanjutnya, log yang terbaca akan dikirimkan ke komponen Logstash menggunakan protokol dan *port* yang telah ditentukan dalam arsitektur sistem. Dalam implementasi ini, pengiriman log ke Elasticsearch dinonaktifkan agar jalur pemrosesan terpusat melalui Logstash, sesuai dengan alur integrasi yang telah dirancang.

Dengan konfigurasi tersebut, setiap aktivitas mencurigakan yang tercatat oleh OpenCanary akan segera diteruskan ke Logstash, yang kemudian akan memproses data dan menyimpannya ke dalam Elasticsearch. Proses ini memungkinkan administrator jaringan untuk mengakses informasi log secara interaktif melalui dashboard Kibana. Penggunaan *Filebeat* dalam penelitian ini terbukti mendukung sistem monitoring secara efisien, aman, dan terintegrasi.

4.2.2 Implementasi ELK Stack

Pada bagian ini dijelaskan tahapan implementasi dan pengujian sistem ELK Stack, yang terdiri atas Elasticsearch, Logstash, dan Kibana, sebagai komponen utama dalam sistem pemantauan keamanan jaringan yang terintegrasi dengan honeypot OpenCanary. ELK Stack dipilih karena kemampuannya dalam mengelola log secara terpusat, mendukung pemrosesan data secara fleksibel, serta menyajikan hasil analisis dalam bentuk visualisasi interaktif yang informatif. Instalasi dan konfigurasi dilakukan pada sebuah *Virtual Private Server* (VPS) berbasis Ubuntu Server 22.04 LTS. Seluruh tahapan dilakukan secara sistematis untuk memastikan masing-masing komponen dapat berfungsi secara optimal dan terintegrasi dalam arsitektur pemantauan jaringan.



Gambar 4.2 Implementasi ELK Stack

Tahapan awal dimulai dengan memperbarui sistem dan menambahkan repositori resmi Elastic agar semua komponen ELK Stack dapat diinstal dari sumber terpercaya. Konfigurasi keamanan dilakukan melalui penambahan kunci autentikasi GPG, serta penyusunan daftar repositori yang mendukung pengunduhan Elasticsearch, Logstash, dan Kibana secara aman dan stabil.

Elasticsearch dikonfigurasi untuk dapat diakses dari luar VPS dan berjalan dalam mode node tunggal, menyesuaikan dengan kebutuhan lingkungan pengujian. Konfigurasi ini memungkinkan sistem untuk menyimpan data log secara terpusat, sekaligus mendukung pencarian dan agregasi data dengan efisien.

Kibana kemudian diinstal dan dikonfigurasi sebagai antarmuka visualisasi yang terhubung langsung dengan Elasticsearch. Pengaturan dilakukan agar antarmuka ini dapat diakses secara publik melalui *browser*, sehingga memudahkan pengguna dalam mengamati dan menganalisis data log secara *real-time* melalui *dashboard* interaktif.

Selanjutnya Logstash dikonfigurasi untuk menerima *input* dari *Filebeat*. Data *log* yang diterima akan difilter dan diproses sebelum dikirimkan ke Elasticsearch dalam bentuk indeks yang diatur secara dinamis berdasarkan tanggal. Konfigurasi ini memungkinkan pengelolaan data log menjadi lebih terstruktur dan mudah dianalisis.

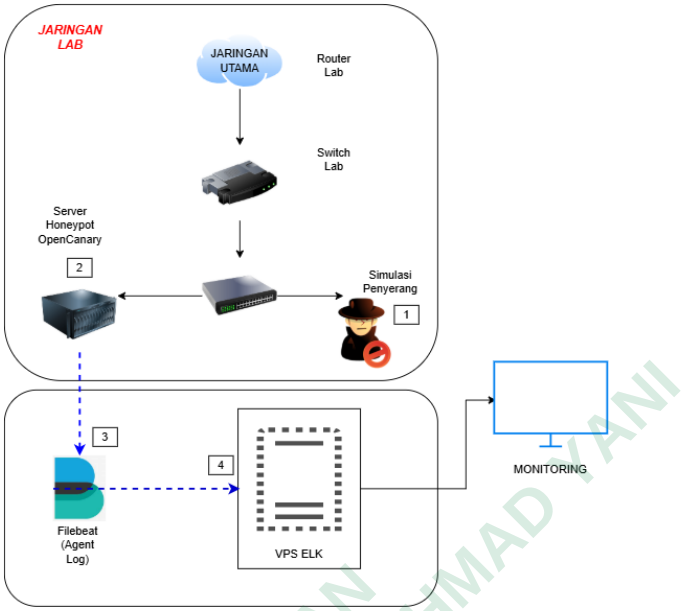
Untuk mendukung konektivitas antar komponen, konfigurasi firewall dilakukan guna membuka *port-port* yang diperlukan, seperti port komunikasi untuk Elasticsearch, Kibana, dan Logstash. Hal ini bertujuan untuk menjamin komunikasi data antar komponen berjalan tanpa hambatan, sekaligus tetap menjaga aspek keamanan sistem.

Langkah terakhir dalam proses implementasi adalah menyusun visualisasi data log melalui Kibana. Setelah indeks berhasil dikenali, pola indeks dibuat dengan nama `OpenCanary-*` untuk mencakup semua data log dari Filebeat. Kibana menyediakan berbagai fitur seperti *Discover, Visualize,* dan *Dashboard* untuk menyajikan data log dalam bentuk grafik linier, diagram batang, donut chart, peta geografis, maupun tabel dinamis. Dengan visualisasi ini, administrator jaringan dapat melakukan analisis mendalam terhadap pola serangan berdasarkan waktu, sumber IP, port yang disasar, hingga jenis aktivitas.

4.2.3 Pengujian Sistem

Pengujian sistem pemantauan keamanan jaringan dilakukan dalam lingkungan jaringan tertutup untuk menilai sejauh mana integrasi antara honeypot OpenCanary dan ELK Stack mampu mendeteksi, mengelola, dan memvisualisasikan aktivitas mencurigakan secara efektif. Pengujian ini penting untuk memastikan bahwa seluruh komponen sistem berfungsi sebagaimana mestinya sebelum diimplementasikan dalam lingkungan jaringan publik yang sesungguhnya.

Lingkungan pengujian disusun dalam skema jaringan laboratorium yang terisolasi dari jaringan kampus utama, guna menjamin keamanan dan kontrol selama proses uji coba. Jaringan ini terdiri dari empat perangkat utama, yaitu: perangkat simulasi penyerang, *server* honeypot OpenCanary, agen *log Filebeat*, dan server ELK Stack berbasis VPS. Setiap perangkat menggunakan sistem operasi Ubuntu Server 22.04 LTS (kecuali perangkat penyerang yang menggunakan Kali Linux) dan dikonfigurasi dengan alamat IP statik, untuk menjamin kestabilan komunikasi antar komponen.



Gambar 4.3 Lingkungan Jaringan Uji

Untuk mendukung proses integrasi dan komunikasi antar komponen dalam sistem, setiap perangkat yang digunakan dalam jaringan uji diberikan alamat IP statis terkecuali alamat IP pada VPS ELK Stack. Penetapan alamat IP ini bertujuan untuk memastikan kestabilan koneksi dan kemudahan dalam proses konfigurasi layanan, serta untuk menghindari terjadinya konflik alamat selama pengujian berlangsung. Adapun rincian alamat IP dan peran masing-masing perangkat dalam jaringan laboratorium dapat dilihat pada tabel berikut:

Tabel 4.1 Tabel IP Perangkat

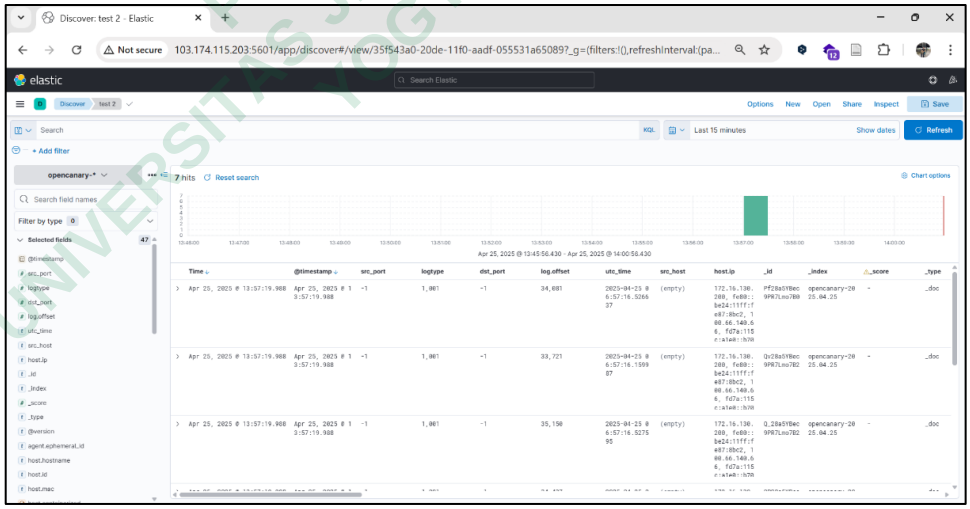
No	Nama Perangkat	Sistem Operasi	Alamat IP	Status IP
1	Simulasi Penyerang	Kali Linux (Virtual Box)	172.16.130.205	IP Private, Static
2	Honeypot OpenCanary	Ubuntu Server 22.04 Lts	172.16.130.200	IP Private, Static
3	Agen Log Filebat	Ubuntu Server 22.04 Lts	172.16.130.200	IP Private, Static
4	Virtual Private Server ELK Stack	Ubuntu Server 22.04 Lts	103.174.115.203	IP Publik

Adapun skema pengujian memposisikan honeypot sebagai target serangan dalam jaringan lokal, sementara *Filebeat* bertugas mengirimkan log aktivitas ke Logstash pada server ELK Stack. Server ELK Stack terdiri dari tiga komponen

utama: Logstash sebagai pemroses log, Elasticsearch sebagai penyimpan data, dan Kibana sebagai alat visualisasi.

Pengujian integrasi dilakukan dengan memanfaatkan perangkat simulasi penyerang yang menjalankan sistem operasi *Kali Lin*ux dan sejumlah alat penetration testing, seperti *Nmap*. Aktivitas penyerangan dilakukan dengan menyasar IP honeypot OpenCanary melalui perintah pemindaian, untuk menguji apakah OpenCanary mampu mendeteksi dan mencatat aktivitas tersebut secara otomatis. Salah satu pengujian yang dilakukan adalah pemindaian *port* menggunakan perintah `nmap 172.16.130.200`, yang bertujuan mengidentifikasi layanan terbuka dan menciptakan jejak aktivitas mencurigakan.

Setelah simulasi serangan dijalankan, honeypot OpenCanary secara otomatis mencatat aktivitas tersebut ke dalam *file log* dalam format JSON. *Filebeat* yang telah dikonfigurasi sebagai agen pengiriman log kemudian membaca file ini dan meneruskannya ke Logstash. Selanjutnya, Logstash memproses *log* menggunakan filter yang telah ditentukan dan mengirimkan data yang telah terstruktur ke Elasticsearch. Data tersebut kemudian dapat divisualisasikan secara *real-time* melalui antarmuka Kibana.



Gambar 4.4 Hasil Deteksi Pada ELK Stack

Hasil dari pengujian menunjukkan bahwa seluruh aktivitas pemindaian yang dilakukan berhasil ditampilkan dalam dashboard Kibana. Informasi yang tercatat meliputi alamat IP penyerang, port yang dipindai, jenis layanan yang

diakses, serta waktu kejadian. Keberhasilan ini membuktikan bahwa integrasi antara honeypot dan ELK Stack berjalan dengan baik dan dapat digunakan untuk mendeteksi serta memantau aktivitas serangan secara efektif dalam waktu nyata.

Dengan demikian, pengujian pada jaringan tertutup ini menjadi validasi awal bahwa sistem mampu menjalankan fungsi utamanya sebagai sistem pemantauan keamanan jaringan. Tahap selanjutnya adalah implementasi sistem dalam lingkungan jaringan publik guna mengamati kinerja sistem pada skenario yang lebih nyata dan kompleks.

4.2.4 Implementasi Pada Jaringan Publik

Setelah sistem pemantauan keamanan jaringan berhasil dibangun dan diuji pada lingkungan laboratorium yang terkontrol, tahap selanjutnya adalah implementasi pada jaringan publik yang sesungguhnya. Langkah ini dilakukan untuk memastikan bahwa sistem dapat beroperasi secara langsung dalam menangani lalu lintas data nyata dari dan menuju jaringan eksternal, serta mampu mendeteksi berbagai potensi ancaman siber yang datang dari luar kampus secara *real-time.*

Implementasi diawali dengan penyesuaian konfigurasi jaringan pada perangkat honeypot yang sebelumnya menggunakan alamat IP privat dalam jaringan lokal, dan kemudian dialihkan ke alamat IP publik. Perubahan ini memungkinkan perangkat honeypot dapat diakses secara langsung melalui koneksi internet publik, sehingga trafik dari luar jaringan dapat terdeteksi dan dicatat secara aktif oleh sistem.

Tabel 4.2 IP Publik Server OpenCanary

Alamat IP	103.247.15.117/29
Subnet Mask	255.255.255.248
Gateway	103.247.15.113
DNS Server	103.247.15.113

Selanjutnya perangkat honeypot secara fisik dipindahkan dari laboratorium ke ruang server utama kampus. Pemindahan ini bertujuan untuk memastikan

perangkat berada dalam lingkungan infrastruktur yang mendukung konektivitas jaringan publik secara stabil dan terus-menerus selama 24 jam. Dengan demikian, perangkat honeypot dapat berfungsi secara optimal sebagai sistem deteksi dini terhadap ancaman yang datang dari luar jaringan kampus.

Dengan telah diterapkannya pengaturan IP publik dan penempatan perangkat pada jaringan utama institusi, sistem pemantauan keamanan jaringan secara resmi mulai beroperasi di lingkungan yang nyata. Implementasi ini menjadi tonggak penting dalam pengawasan aktif terhadap lalu lintas jaringan publik, sekaligus menjadi bagian integral dari strategi peningkatan keamanan siber di lingkungan Universitas Jenderal Achmad Yani Yogyakarta.

4.3 Pembahasan

4.3.1 Periode *Monitoring*

Tahap *monitoring* merupakan fase penting dalam evaluasi sistem pemantauan keamanan jaringan yang telah diimplementasikan. Tujuan utama dari *monitoring* ini adalah mengamati performa sistem dalam mendeteksi dan merekam aktivitas jaringan, terutama terhadap ancaman siber yang potensial. Sistem yang dibangun diamati secara berkelanjutan guna memperoleh data log yang representatif dan mendeteksi pola-pola serangan yang muncul melalui interaksi dengan layanan honeypot.

Proses *monitoring* dilakukan dengan memanfaatkan antarmuka Kibana, yang menampilkan log aktivitas dari OpenCanary melalui integrasi sistem ELK Stack. Selama periode ini, dilakukan observasi terhadap berbagai bentuk aktivitas mencurigakan, seperti upaya login tidak sah, pemindaian port, dan interaksi abnormal terhadap layanan palsu yang disimulasikan. Setiap kejadian yang terekam akan dianalisis lebih lanjut untuk memahami karakteristik serangan yang masuk.

Penentuan durasi monitoring didasarkan pada dua pertimbangan utama, yaitu kapasitas penyimpanan sistem dan kebutuhan administratif penelitian. Berdasarkan observasi awal pada tanggal 1 dan 2 Mei 2025, rata-rata pertumbuhan data log mencapai sekitar 0,2 GB per hari. Dengan kapasitas penyimpanan *server* sebesar 20 GB, serta mempertimbangkan alokasi sistem dan buffer internal, estimasi ruang efektif yang tersedia untuk penyimpanan log berkisar antara 10

hingga 13 GB. Berdasarkan estimasi ini, durasi monitoring maksimum dapat mencapai sekitar 50 hari tanpa mengganggu kinerja sistem.

Namun demikian, dalam konteks penelitian ini, periode monitoring ditetapkan selama 30 hari. Penetapan ini mempertimbangkan aspek administratif, seperti tenggat waktu pengumpulan data dan penyusunan laporan tugas akhir. Durasi ini dinilai memadai untuk memperoleh data serangan yang cukup representatif, sekaligus memberikan ruang waktu yang cukup untuk proses analisis dan dokumentasi hasil penelitian secara menyeluruh.

Selama periode 30 hari tersebut, sistem honeypot OpenCanary secara aktif mencatat semua aktivitas terhadap layanan yang disimulasikan, kemudian mengirimkan log ke ELK Stack untuk diproses dan divisualisasikan. Proses ini memberikan gambaran utuh terhadap intensitas serangan, sumber ancaman, serta kecenderungan pola serangan yang terjadi selama sistem dijalankan dalam lingkungan jaringan publik.

4.3.2 Statistik Umum Aktivitas Jaringan

Selama periode monitoring selama 30 hari, sistem honeypot OpenCanary yang telah diimplementasikan pada jaringan publik berhasil merekam berbagai aktivitas mencurigakan dari lingkungan eksternal. Seluruh log yang tertangkap dikirim secara otomatis ke sistem ELK Stack untuk diproses dan divisualisasikan melalui antarmuka Kibana. Berdasarkan hasil pemantauan, tercatat intensitas aktivitas serangan yang bervariasi setiap harinya, dengan kecenderungan konsisten terhadap layanan-layanan tertentu yang umumnya menjadi sasaran eksploitasi. Tabel berikut merangkum statistik umum dari hasil monitoring selama periode tersebut:

Tabel 4.3 Tabel Statistik Umum

No	Kategori Statistik	Nilai
1	Jumlah Total Log Tercatat	2.209.032
2	Rata-Rata Log per Hari	73.634 rata-rata serangan perhari

No	Kategori Statistik	Nilai
3	Hari dengan Aktivitas Tertinggi	124.544 log pada tanggal 29 Mei 2025 pukul 00:00
4	Hari dengan Aktivitas Terendah	5.309 log pada tanggal 18 Mei 2025 pukul 12:00
5	Port Tujuan Paling Sering Diserang	3389 (Port Remote Dekstop Protokol (RDP)), 1433 (Port Microsoft SQL server), 22 (Port SSH)
6	Kategori Aktivitas Paling Dominan	SMTP Login Attempt
7	Username Paling Sering dicoba	Hello (580.741 Percobaan), 103 (87.983 percobaan), root (62.518 percobaan)
8	IP sumber yang paling sering muncul	101.227.104.13. (328.260 Serangan).
9	Negara Asal Penyerang terbanyak	Vietnam

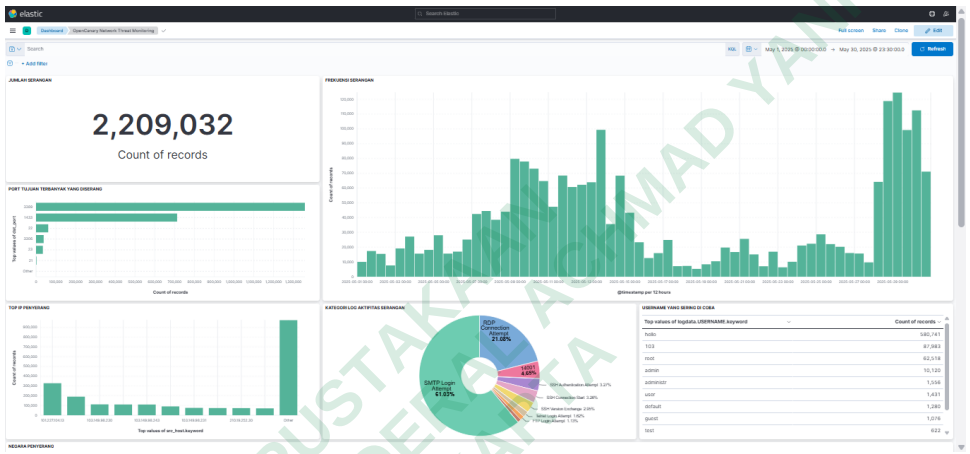
Statistik tersebut menunjukkan bahwa sistem honeypot berfungsi secara efektif dalam mendeteksi dan mencatat serangan siber yang terjadi dalam skala besar. Dominasi aktivitas terhadap layanan SMTP, serta serangan berulang ke *port* kritikal seperti RDP dan SQL Server, mengindikasikan tingginya intensitas serangan otomatis yang dilakukan oleh skrip masif atau jaringan *botne*t. Temuan ini memperkuat pentingnya pemantauan jaringan secara *real-time* dalam mendeteksi dan menganalisis potensi ancaman sebelum berkembang menjadi insiden yang lebih serius.

4.3.3 Visualisasi Data Hasil Monitoring

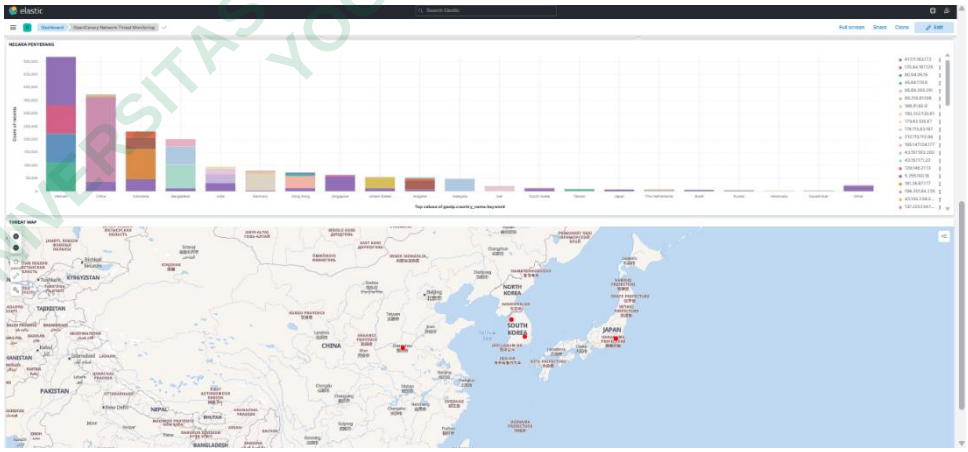
Untuk memperkuat pemahaman terhadap data hasil pemantauan yang telah dikumpulkan selama 30 hari, dilakukan visualisasi berbasis *dashboard* Kibana. Visualisasi ini disusun berdasarkan parameter-parameter penting yang mencakup tren aktivitas harian, IP sumber serangan, *port* tujuan, pola *username* yang digunakan dalam upaya *login* tidak sah, hingga kategori dan asal negara aktivitas mencurigakan. Pendekatan visual ini bertujuan untuk menyajikan data secara lebih

informatif, membantu identifikasi pola serangan, serta mendukung pengambilan keputusan dalam strategi pengamanan jaringan.

Gambar berikut menunjukkan tampilan keseluruhan dashboard monitoring berbasis Kibana yang digunakan dalam penelitian ini. Dashboard ini terdiri dari beberapa panel yang menampilkan statistik log serangan, negara asal penyerang, alamat IP sumber, serta pola aktivitas mencurigakan lainnya yang terekam selama proses pemantauan.



Gambar 4.5 Dashboard Kibana - Bagian Atas



Gambar 4.6 Dashboard Kibana - Bagian Bawah

A. Rekap Harian Aktivitas Serangan

Rekap harian disusun dalam bentuk tabel untuk menunjukkan fluktuasi jumlah log, IP sumber dominan, dan port yang paling sering ditargetkan setiap harinya.

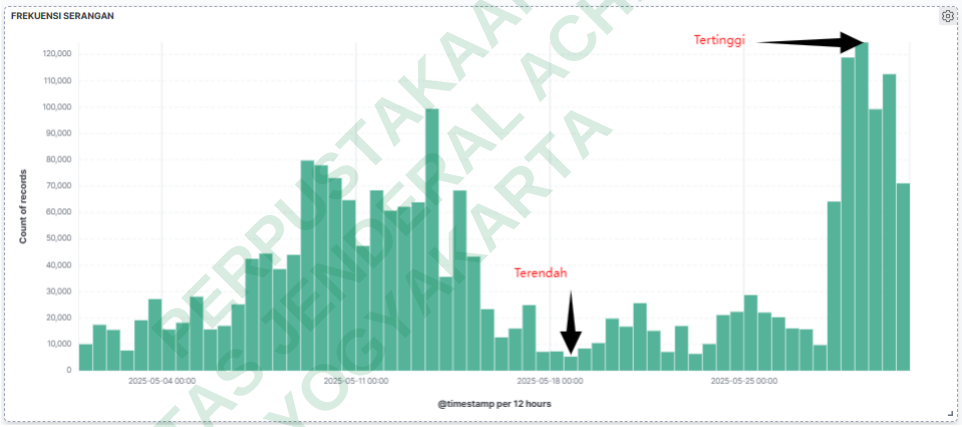
Tabel 4.4 Rekap Harian Aktivitas Serangan

Tanggal	Jumlah Log	IP sumber dominan	Port Tujuan Dominan
1 Mei 2025	27.273 log	103.247.123.58	1433 (SQL Server)
2 Mei 2025	22.978	38.148.241.22	1433 (SQL Server)
3 Mei 2025	46.097	103.247.123.58	1433 (SQL Server)
4 Mei 2025	30.0556	38.148.242.51	1433 (SQL Server)
5 Mei 2025	39.542	103.247.123.58	1433 (SQL Server)
6 Mei 2025	37.451	203.124.40.95	1433 (SQL Server)
7 Mei 2025	85.702	103.247.123.58	3389 (RDP)
8 Mei 2025	80.041	103.149.96.230	3389 (RDP)
9 Mei 2025	154.262	103.149.96.230	3389 (RDP)
10 Mei 2025	136.253	103.149.98.242	3389 (RDP)
11 Mei 2025	113.427	103.149.98.242	3389 (RDP)
12 Mei 2025	120.698	103.149.98.242	3389 (RDP)
13 Mei 2025	160.560	103.149.98.231	3389 (RDP)
14 Mei 2025	101.813	103.189.237.64	3389 (RDP)
15 Mei 2025	65.963	103.189.237.64	3389 (RDP)
16 Mei 2025	28.164	103.149.98.233	3389 (RDP)
17 Mei 2025	31.829	103.149.98.233	3389 (RDP)
18 Mei 2025	12.548	221.179.236.82	1433 (SQL Server)
19 Mei 2025	18.783	103.247.123.58	1433 (SQL Server)
20 Mei 2025	36.414	103.189.237.64	3389 (RDP)
21 Mei 2025	40.684	112.213.101.23	3389 (RDP)
22 Mei 2025	23.314	103.247.123.58	1433 (SQL Server)
23 Mei 2025	15.628	163.47.35.89	3389 (RDP)
24 Mei 2025	42.558	163.47.35.89	3389 (RDP)
25 Mei 2025	49.618	163.47.35.89	3389 (RDP)
26 Mei 2025	35.473	163.47.35.89	3389 (RDP)
27 Mei 2025	24.713	103.101.226.102	3389 (RDP)
28 Mei 2025	179.044	101.227.104.13	1433 (SQL Server)
29 Mei 2025	220.511	101.227.104.13	1433 (SQL Server)
30 Mei 2025	183.589	101.227.104.13	1433 (SQL Server)

Analisis terhadap data tersebut menunjukkan bahwa pola serangan bersifat fluktuatif namun konsisten dalam menargetkan port kritikal seperti 3389 (RDP), 1433 (SQL Server), dan 22 (SSH). Kecenderungan munculnya IP sumber yang sama secara berulang memperkuat indikasi adanya aktivitas otomatis dari botnet atau skrip serangan massal.

B. Grafik Tren Harian Aktivitas Serangan

Grafik tren harian serangan menyajikan jumlah log yang tercatat setiap hari selama proses monitoring berlangsung. Dari grafik ini terlihat bahwa terdapat fluktuasi jumlah serangan dari hari ke hari, dengan tren yang cenderung meningkat pada waktu-waktu tertentu.



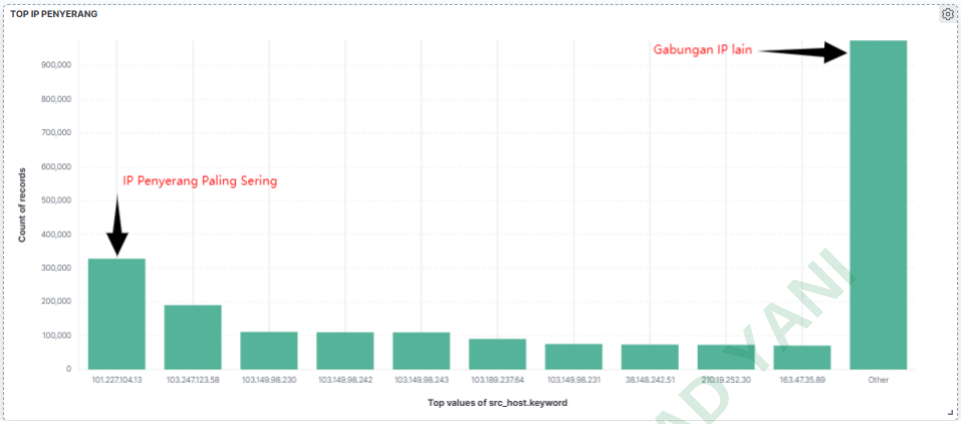
Gambar 4.7 Visualisasi Frekuensi Serangan

Grafik menunjukan bahwa puncak serangan terjadi pada tanggal 29 Mei 2025 dengan 124.544 log, sedangkan serangan paling rendah tercatat pada 18 Mei 2025 dengan 5.309 log. Lonjakan aktivitas tersebut dapat menjadi indikator adanya serangan terkoordinasi atau aktivitas dari botnet pada waktu-waktu tertentu. Fluktuasi ini menunjukkan bahwa sistem harus tetap aktif dan waspada sepanjang waktu karena pola serangan tidak selalu stabil.

C. Grafik IP Penyerang Terbanyak

Grafik ini menunjukan sepuluh alamat IP yang paling sering muncul sebagai sumber aktivitas mencurigakan selama proses monitoring. Informasi ini sangat penting untuk proses penilaian potensi ancaman,

terutama jika IP tersebut muncul secara konsisten dan berasal dari negara tertentu.

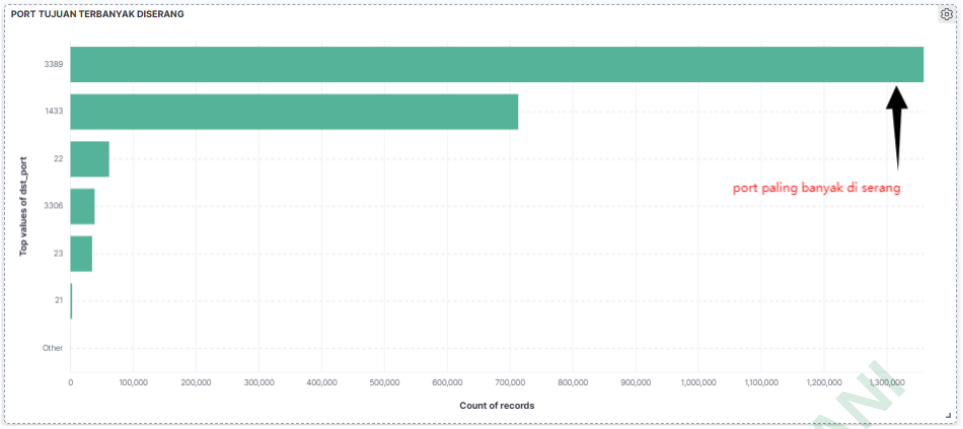


Gambar 4. 8 Visualisasi Grafik Top IP Penyerang

Hasil analisis menunjukkan bahwa IP 101.227.104.13 tercatat sebagai sumber serangan terbanyak dengan 307.339 aktivitas, disusul oleh IP lain seperti 103.247.123.58 dan 103.149.98.230. Mayoritas IP ini berasal dari wilayah geografis yang sama dan sering digunakan dalam serangan otomatis. Dengan memanfaatkan fitur GeoIP di dashboard Kibana, alamat-alamat IP tersebut juga dapat dipetakan secara geografis untuk analisis spasial lebih lanjut.

D. Grafik Distribusi Port Tujuan

Port tujuan yang diserang memberikan wawasan tentang layanan atau protokol jaringan yang menjadi target utama dari aktivitas penyerangan. Grafik ini membantu mengidentifikasi layanan mana yang paling rentan dieksploitasi.



Gambar 4. 9 Visualisasi Port Tujuan Terbanyak diserang

Berdasarkan grafik yang dihasilkan, port 3389 (Remote Desktop Protocol - RDP) tercatat sebagai port yang paling sering diserang, diikuti oleh port 1433 (Microsoft SQL Server) dan port 22 (Secure Shell - SSH)**.** Pola ini sejalan dengan tren global, di mana port-port yang terkait dengan akses jarak jauh dan *database* menjadi target utama dari serangan brute-force dan eksploitasi kerentanan.

E. *Username* Pada Upaya Login Tidak Sah

Tabel 4.5 menunjukkan frekuensi penggunaan username tertentu dalam upaya login yang terekam oleh honeypot. Data ini memberikan gambaran mengenai strategi *brute-force* yang digunakan penyerang.

Tabel 4.5 Username Pada Upaya Login Tidak Sah

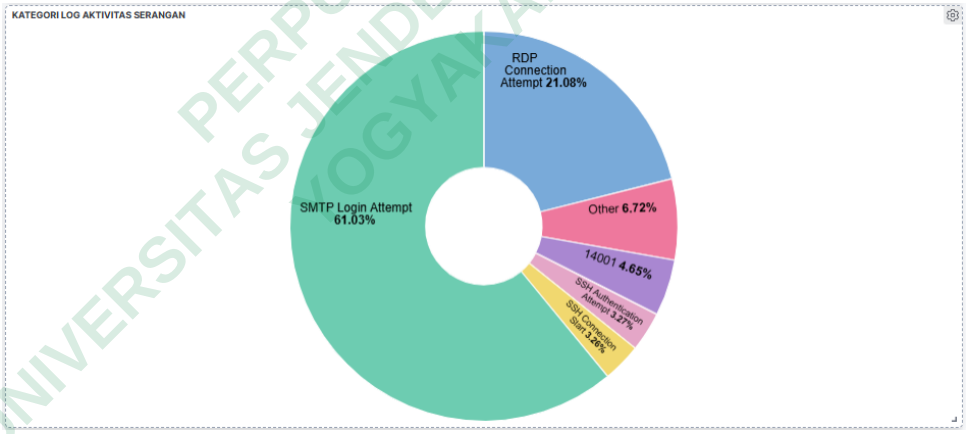
No	Username	Jumlah Percobaan
1	hello	580.741
2	103	87.983
3	root	62.518
4	admin	10.120
5	administr	1.556
6	user	1.431
7	default	1.280
8	guest	1.076
9	test	622

No	Username	Jumlah Percobaan
10	support	544
11	other	27.150

Tercatat bahwa username `hello` digunakan dalam 578.984 percobaan login, disusul oleh `103` sebanyak 87.983 kali dan `root` sebanyak 63.515 kali. Username-username ini menunjukkan bahwa penyerang tidak hanya menargetkan akun default sistem (seperti `root`), tetapi juga menggunakan pola acak yang kemungkinan dihasilkan oleh skrip otomatis. Informasi ini sangat berguna dalam menyusun kebijakan hardening akun dan sistem autentikasi di lingkungan jaringan sebenarnya.

F. Visualisasi Kategori Aktivitas Serangan

Visualisasi ini menampilkan proporsi berbagai jenis aktivitas serangan yang tercatat selama proses monitoring berdasarkan nilai field `logtype`. Setiap `logtype` merepresentasikan kategori aktivitas yang terjadi.



Gambar 4. 10 Kategori Log Aktivitas Serangan

Hasil visualisasi menunjukkan bahwa jenis serangan yang paling dominan adalah percobaan login SMTP dan akses tidak sah ke layanan SSH**,** masing-masing dengan persentase yang cukup signifikan dari total log. Donut chart ini memberikan gambaran yang jelas mengenai fokus utama serangan terhadap sistem, serta variasi jenis interaksi mencurigakan yang dilakukan oleh penyerang. Informasi ini penting untuk menentukan prioritas

respons keamanan dan memperkuat layanan yang paling rentan dieksploitasi.

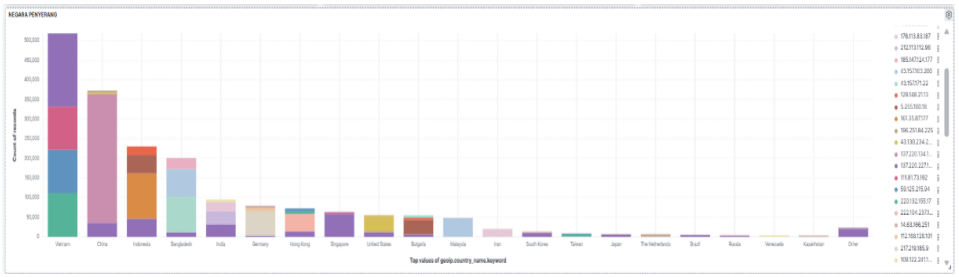
Untuk memperjelas distribusi kuantitatif dari setiap kategori serangan, berikut disajikan sampel log berdasarkan jenis logtype yang tercatat selama periode pemantauan.

Tabel 4.6 Sampel Log Berdasarkan Jenis Logtype

@timestamp	logtype
May 28, 2025 @ 16:57:08.708	RDP Connection Attempt
May 28, 2025 @ 16:57:08.708	RDP Connection Attempt
May 28, 2025 @ 16:57:08.708	SMTP Login Attempt
May 28, 2025 @ 16:57:08.708	SMTP Login Attempt
May 28, 2025 @ 16:57:08.707	SMTP Login Attempt
May 28, 2025 @ 16:57:06.705	RDP Connection Attempt
May 28, 2025 @ 16:57:06.705	RDP Connection Attempt
May 28, 2025 @ 16:57:06.705	SMTP Login Attempt
May 28, 2025 @ 16:57:06.705	SMTP Login Attempt
May 28, 2025 @ 16:57:06.705	SMTP Login Attempt
May 28, 2025 @ 11:12:37.918	RDP Connection Attempt
May 28, 2025 @ 11:12:37.917	SMTP Login Attempt
May 28, 2025 @ 11:12:37.917	SMTP Login Attempt
May 28, 2025 @ 11:12:37.917	SMTP Login Attempt
May 28, 2025 @ 11:12:36.917	SMTP Login Attempt
May 28, 2025 @ 11:12:36.917	SMTP Login Attempt
May 28, 2025 @ 11:12:36.916	SMTP Login Attempt
May 28, 2025 @ 16:57:05.705	RDP Connection Attempt

G. Visualisasi Negara Asal Serangan

Grafik ini menunjukkan tren harian aktivitas serangan yang berasal dari masing-masing negara selama 30 hari *monitoring*. Data dihasilkan melalui field `geoip.country_name.keyword` yang ditambahkan melalui *plugin* `geoip` pada pipeline Logstash.



Gambar 4.11 Negara Penyerang

Visualisasi ini memperlihatkan bahwa negara dengan jumlah aktivitas tertinggi adalah Vietnam**,** diikuti oleh Rusia dan Tiongkok**,** dengan fluktuasi yang terjadi secara periodik. Kenaikan tajam aktivitas dari negara tertentu pada hari-hari tertentu dapat menunjukkan adanya kampanye serangan terkoordinasi atau perubahan pola penyerang.

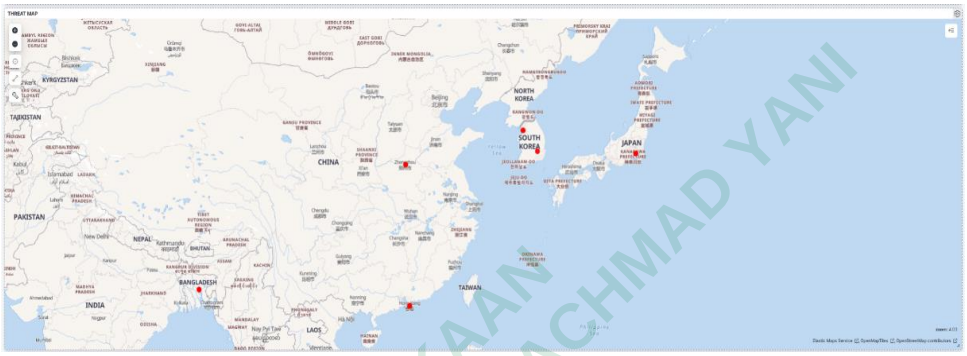
Sebagai pelengkap dari visualisasi grafik, tabel 4.7 menyajikan daftar alamat IP yang terdeteksi berasal dari masing-masing negara penyerang. Tabel tersebut memberikan rincian lebih spesifik mengenai distribusi IP yang menjadi sumber serangan, sehingga dapat memperkuat analisis terhadap asal geografis aktivitas berbahaya yang terpantau selama periode *monitoring*. Data ini dihasilkan dari hasil ekstraksi *field* geoip melalui pipeline Logstash, yang mengaitkan setiap alamat IP dengan negara asalnya.

Tabel 4.7 Tabel IP Negara Penyerang

No	Asal Negara	Alamat IP
1	Vietnam	103.149.98.230, 103.149.98.242, 103.149.98.243,
2	China	117.187.125.174, 123.138.18.10, 101.227.104.13,
3	Indonesia	158.140.181.138, 103.101.226.102, 103.247.123.58,
4	Bangladesh	163.47.35.91, 163.47.35.89, 103.189.237.64,
5	…..	…..
6	…..	…..
7	…..	…..
8	Kazakstan	45.84.178.8, 95.58.255.251, 89.218.81.106

H. Peta Lokasi Penyerang

Sebagai pelengkap visualisasi pada *dashboard*, digunakan peta koordinat (GeoIP map) untuk menunjukkan sebaran geografis alamat IP yang melakukan serangan. Visualisasi ini ditampilkan melalui fitur *coordinate map* atau *region map* di Kibana, menggunakan data `geoip.location`.



Gambar 4.12 Lokasi Negara Penyerang

Peta ini menampilkan titik-titik lokasi yang merepresentasikan asal alamat IP sumber serangan. Titik-titik terkonsentrasi di kawasan Asia dan Eropa Timur, dengan warna atau ukuran yang menunjukkan volume serangan dari wilayah tersebut. Threat map ini memberikan cara intuitif bagi administrator jaringan untuk memahami distribusi global ancaman dan mengidentifikasi area geografis yang menjadi pusat serangan siber terhadap sistem UNJAYA.

4.3.4 Analisis Pola Serangan

Analisis pola serangan dilakukan untuk mengidentifikasi tren, kecenderungan, serta karakteristik ancaman yang terekam selama periode monitoring. Tujuan dari analisis ini adalah menginterpretasikan data log yang telah disajikan dalam bentuk statistik dan visualisasi, guna memahami pola aktivitas mencurigakan serta potensi risiko yang ditimbulkan terhadap sistem. Pendekatan analisis dilakukan berdasarkan dimensi waktu kejadian, *port* tujuan, alamat IP sumber, negara asal, *username* yang digunakan, serta kategori aktivitas yang tercatat oleh sistem honeypot OpenCanary.

A. Pola Berdasarkan Frekuensi Waktu

Selama 30 hari masa monitoring, sistem honeypot OpenCanary secara konsisten mencatat aktivitas serangan setiap hari, dengan intensitas yang sangat bervariasi. Jumlah log tertinggi tercatat pada 29 Mei 2025 sebesar 220.511 entri, sementara jumlah terendah terjadi pada 18 Mei 2025 sebanyak 12.548 log. Fluktuasi ini tidak menunjukkan pola mingguan yang jelas, namun tampak adanya lonjakan signifikan pada pertengahan hingga akhir bulan yang mengindikasikan aktivitas serangan berskala besar, kemungkinan berasal dari kampanye botnet.

Berdasarkan observasi melalui dashboard Kibana, aktivitas serangan tersebar merata sepanjang hari tanpa adanya periode hening. Terdapat kecenderungan peningkatan aktivitas pada rentang waktu dini hari (sekitar pukul 00.00–07.00), yang memperkuat indikasi bahwa mayoritas serangan dilakukan oleh sistem otomatis atau *botnet* yang beroperasi lintas zona waktu. Temuan ini menegaskan bahwa ancaman siber bersifat persisten, acak, dan berlangsung sepanjang waktu, sehingga sistem pemantauan perlu beroperasi secara aktif dan adaptif setiap saat.

B. Pola Berdasarkan Port Tujuan

Hasil pemantauan menunjukkan bahwa serangan secara konsisten menargetkan port-port tertentu yang dianggap kritikal. Tiga port utama yang paling sering menjadi sasaran adalah:

1. Port 3389 (RDP): digunakan untuk akses jarak jauh pada sistem Windows. Frekuensi tinggi terhadap port ini mengindikasikan upaya pengambilalihan kendali sistem melalui remote desktop.
2. Port 1433 (Microsoft SQL Server): menunjukan upaya eksploitasi terhadap sistem basis data, baik melalui kerentanan layanan maupun percobaan login dengan kredensial default.

3. Port 22 (SSH): umum ditemukan pada sistem Linux/Unix dan sering menjadi target *brute-force login* untuk mendapatkan hak akses administratif.

Fokus serangan pada port-port ini menggambarkan kecenderungan penyerang untuk mengeksploitasi layanan administratif dan basis data, yang jika berhasil diakses dapat memberikan kontrol penuh terhadap sistem.

C. Pola Berdasarkan Alamat IP dan Asal Negara

Sistem honeypot OpenCanary berhasil merekam ribuan alamat IP sebagai sumber serangan. Tiga alamat IP dengan intensitas tertinggi adalah:

1. 101.227.104.13 sebanyak 328.260 log
2. 103.247.123.58 sebanyak 190.687 log
3. 103.149.98.230 sebanyak 111.427 log

Munculnya IP yang sama secara berulang menunjukkan adanya pola serangan yang bersifat otomatis dan persisten, kemungkinan besar dijalankan oleh botnet atau skrip otomatis dari server tertentu.

Secara geografis, hasil pemetaan GeoIP menunjukkan bahwa sebagian besar serangan berasal dari Vietnam, diikuti oleh Tiongkok dan Indonesia. Konsentrasi aktivitas di wilayah Asia Timur dan Asia Tenggara menjadi pertimbangan penting dalam menyusun kebijakan mitigasi risiko berbasis lokasi, seperti pemfilteran IP atau pengawasan terhadap trafik internasional tertentu.

D. Pola Berdasarkan *Username*

Sistem mencatat ribuan upaya login terhadap layanan yang disimulasikan. Username yang paling sering digunakan dalam serangan antara lain:

1. hello**:** 590.741 kali.
2. 103: 87.983 kali.
3. root**:** 63.518 kali.

Penggunaan nama acak dan umum seperti “hello” dan “103” mengindikasikan pemanfaatan *wordlist* otomatis oleh penyerang, sementara penggunaan “root” menunjukkan upaya eksploitasi akun default sistem.

Temuan ini menunjukkan bahwa teknik *brute-force* login masih menjadi metode yang dominan, dan menekankan pentingnya penerapan kebijakan keamanan seperti pembatasan upaya *login*, penghapusan akun default, serta autentikasi multi-faktor.

E. Pola Berdasarkan Kategori Aktivitas

Setiap aktivitas yang dicatat oleh sistem diklasifikasikan berdasarkan jenis interaksinya menggunakan field `logtype`. Hasil analisis menunjukkan bahwa:

1. SMTP Login Attempt merupakan kategori yang paling dominan
2. Disusul oleh SSH Login Attempt**,**
3. FTP Access Attempt,
4. dan HTTP Access/Scan**.**

Kecenderungan serangan yang bersifat autentikatif menunjukkan bahwa penyerang tidak sekadar melakukan pemindaian (*scanning*), melainkan berupaya aktif untuk mendapatkan akses sistem. Pola ini memberikan gambaran bahwa sebagian besar ancaman yang dihadapi merupakan upaya eksploitasi yang serius, bukan hanya pengintaian pasif.

Berdasarkan analisis pola serangan, dapat disimpulkan bahwa sistem honeypot yang terintegrasi dengan ELK Stack telah mampu mendeteksi dan mencatat berbagai bentuk ancaman siber secara efektif. Aktivitas yang terekam menunjukkan karakteristik serangan yang persisten, bersifat otomatis, dan menargetkan layanan-layanan penting seperti SSH, RDP, dan SQL Server. Data yang diperoleh dari dimensi waktu, *port*, IP sumber, asal negara, *username*, dan kategori aktivitas memberikan dasar yang kuat dalam menyusun kebijakan keamanan yang lebih adaptif, berbasis risiko, serta prediktif terhadap potensi ancaman di masa mendatang.

4.3.5 Kesimpulan Hasil Monitoring

Berdasarkan kegiatan monitoring yang dilakukan selama 30 hari penuh terhadap sistem honeypot OpenCanary yang terintegrasi dengan ELK Stack, dapat

disimpulkan bahwa sistem pemantauan keamanan jaringan yang dibangun telah mampu berfungsi secara efektif, *real-time*, dan responsif dalam mendeteksi serta merekam berbagai aktivitas mencurigakan di jaringan publik.

Selama periode pengamatan, sistem mencatat total sebanyak 2.209.032 entri log, dengan rata-rata sekitar 73.634 log per hari, yang mencerminkan tingginya intensitas dan konsistensi ancaman siber terhadap sistem terbuka. Pola serangan yang terekam menunjukkan karakteristik yang bersifat otomatis**,** persisten, dan berlangsung sepanjang waktu, dengan konsentrasi tertinggi pada port layanan umum seperti RDP (3389)**,** SQL Server (1433)**,** dan SSH (22)**.**

sebagian besar serangan berasal dari alamat IP yang berulang, yang secara geografis didominasi oleh negara Vietnam, diikuti oleh Tiongkok dan Indonesia. Pada aspek autentikasi, penggunaan *username* generik seperti *hello*, *103*, dan *root* mendukung temuan bahwa metode *brute-force login* merupakan teknik serangan yang paling umum digunakan.

Dari segi kategori aktivitas, percobaan login pada layanan SMTP merupakan bentuk serangan yang paling dominan, diikuti oleh upaya akses ke layanan SSH dan FTP. Hal ini menunjukkan bahwa sebagian besar serangan memiliki tujuan eksplisit untuk memperoleh akses tidak sah, bukan sekadar melakukan pemindaian pasif.

Secara keseluruhan, proses monitoring ini membuktikan bahwa sistem yang diimplementasikan mampu memberikan visibilitas yang kuat terhadap potensi ancaman, mengelola log secara terstruktur, serta menyajikan informasi dalam bentuk visualisasi interaktif dan informatif melalui dashboard Kibana. Temuan ini menjadi landasan strategis dalam analisis risiko serta penyusunan kebijakan penguatan keamanan jaringan di lingkungan Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA) secara lebih adaptif dan berbasis data.

4.4 Manajemen Sistem

Tahap manajemen sistem merupakan langkah akhir dalam implementasi sistem pemantauan keamanan jaringan. Tujuan utama dari tahap ini adalah untuk melakukan evaluasi dan penyesuaian terhadap sistem berdasarkan hasil monitoring

serta performa aktual selama sistem dijalankan pada jaringan publik. Evaluasi dilakukan dengan meninjau akurasi log yang ditangkap oleh honeypot, efektivitas visualisasi melalui ELK Stack, serta kestabilan sistem secara keseluruhan.

Berdasarkan hasil observasi selama proses implementasi dan monitoring, dilakukan beberapa tindakan penyesuaian untuk memastikan sistem dapat beroperasi secara optimal. Adapun penyesuaian yang dilakukan meliputi:

A. Penambahan Field GeoIP

Untuk meningkatkan nilai informatif dari data log yang ditampilkan, dilakukan penambahan *field* geoip dalam konfigurasi *pipeline* Logstash. *Field* ini berfungsi untuk mengekstrak informasi geografis berdasarkan alamat IP sumber serangan. Dengan penambahan ini, data log tidak hanya mencatat alamat IP dan port, tetapi juga mencantumkan asal negara atau wilayah IP penyerang, sehingga analisis spasial terhadap pola serangan dapat dilakukan dengan lebih mendalam.

B. Penyesuaian Spesifikasi VPS ELK Stack

Selama implementasi awal, ditemukan bahwa sistem ELK Stack mengalami keterlambatan proses dan gangguan stabilitas layanan, terutama ketika menerima volume log yang tinggi. Setelah dilakukan penelusuran, diketahui bahwa permasalahan disebabkan oleh keterbatasan kapasitas RAM pada server VPS, yang awalnya hanya memiliki memori sebesar 4 GB. Sebagai solusi, kapasitas RAM ditingkatkan menjadi 8 GB. Hasil penyesuaian ini menunjukkan peningkatan performa yang signifikan, di mana layanan Elasticsearch dan Kibana dapat berjalan dengan lebih stabil tanpa mengalami *crash* saat memproses data dalam jumlah besar.

C. Perubahan Alamat IP Publik pada Server Honeypot

Selama proses monitoring berlangsung, dilakukan penyesuaian alamat IP publik pada server honeypot OpenCanary guna mengikuti kebijakan jaringan institusi. Sebelumnya, perangkat honeypot OpenCanary menggunakan alamat 103.247.15.117/29, yang kemudian dialihkan menjadi 103.247.15.118/29. Konfigurasi ini tetap berada dalam subnet yang sama, yakni 255.255.255.248,

dengan gateway 103.247.15.113, sehingga tidak memerlukan perubahan arsitektur jaringan secara menyeluruh.

Dengan dilaksanakannya manajemen sistem secara aktif, kestabilan dan efektivitas sistem pemantauan keamanan jaringan dapat tetap terjaga. Tindakan penyesuaian yang dilakukan bersifat responsif terhadap kondisi nyata selama proses implementasi dan monitoring berlangsung, sekaligus menjadi langkah penting dalam memastikan bahwa sistem tetap relevan terhadap tantangan keamanan siber yang terus berkembang.