BAB 1
PENDAHULUAN

Bab 1 Pendahuluan merupakan bagian awal bab yang memuat latar belakang, rumusan masalah, tujuan, manfaat, batasan masalah, dan sistematika penulisan. Pada bagian ini dijelaskan alasan dari dilakukannya penelitian ini.

1.1 Latar belakang

Perkembangan teknologi semakin pesat di era digital seperti saat ini. Perkembangan teknologi ternyata tidak hanya membawa dampak positif namun juga mengakibatkan munculnya dampak negatif salah satunya yaitu banyaknya serangan yang muncul akibat perkembangan teknologi. Badan Siber dan Sandi Negara (BSSN) pada tahun 2023 mengeluarkan laporan bahwa sepanjang tahun 2022 terdapat anomaly serangan siber di Indonesia sebanyak 976.429.996 dengan 10 jumlah aktivitas terbanyak yaitu *MyloBot Botnet, MinningPool Other Malware, Microsoft windows smb server information disclosure, Generic Trojan RAT, Discover the communication behavior of VPN tool OpenVPN, Discovery using SOCKS agent, Discovery of server information detected via OPTIONS, Plaintext password transmission found, PhishingSite Other Malware*, dan *RDP account brute force guess* (BSSN, 2023).

Meskipun jumlah total tersebut disebutkan bahwa setiap bulan mengalami penurunan, namun bukan hal yang mustahil jika seiring dengan perkembangan teknologi yang semakin pesat jumlah serangan siber juga akan dapat meningkat. Salah satu perkembangan teknologi yang saat ini sedang marak yaitu penggunaan teknologi *cloud* dalam segala bidang. *Cloud Computing* merupakan teknologi tranfsromatif yang berpotensi untuk memberikan kemudahan. *Cloud Computing* dikembangkan sebagai solusi untuk mengatasi berbagai macam permasalahan pada sistem komputer. Teknologi *cloud* telah diadopsi secara luas di segala sektor kehidupan, *cloud* memberikan berbagai macam keuntungan yang membebaskan administrator dari permasalahan perangkat keras seperti skalabilitas, ketersediaan, dan dapat diakses dari mana saja tidak ada batasan geografis (Merin Sam & Kumar T, 2016). Namun seiring dengan perkembangan

cloud, ternyata *Cloud Computing* juga memiliki berbagai macam permasalahan seperti keamanan data pelanggan dan integritas data (Neware & Khan, 2018).

Pada tahun 2022 Open Web Application Security Project (OWASP) mengeluarkan 10 daftar kerentanan pada *Cloud-Native*, kerentanan tersebut antara lain *Insecure cloud configuration (publicly open cloud storage buckets, improper permissions set on cloud storage buckets, container runs as root), injection flaws (sql injection, XXE, NoSQL Injection, OS Command injection), Improper authentication and authorization, CI/CD pipeline and software supply chain flaws, insecure secrets storage, over-permissive or insecure network policies, using components with knows vulnerabilities, improper assets management, inadequate resource quota limits,* dan *ineffective logging and monitoring* (Segal et al., 2022).

Dengan kemudahan yang ditawarkan *cloud computing*, ternyata berbagai macam serangan telah mengintai. Serangan dan ancaman tersebut menimbulkan tantangan dalam pengumpulan barang bukti serangan atau insiden dalam proses digital forensik dan insiden renspons (Neware & Khan, 2018). Pada tahun 2020, Murat dkk melakukan penelitian terkait dengan penanganan insiden pada *cloud environment*, pada penelitian tersebut mengangkat permasalahan terkait dengan tantangan pengumpulan data pada *cloud environment*. Penelitian tersebut mengusulkan penambahan langkah penanganan insiden yang terdapat pada SANS Incident Response Framework. Langkah yang ditambahkan berupa langkah *cloud configuration* pada tahap awal, sehingga tahap penanganan insiden menjadi yang semula terdapat 6 tahap menjadi 7 tahap yaitu *cloud configuration, preparation, identification, containment, eradication, recovery*, dan *lesson learned* (Ozer et al., 2020)(Kral, 2011). Pada penelitian tersebut selain mengusulkan penambahan langkah penanganan insiden juga memberikan solusi dalam melakukan penanganan insiden. Solusi penanganan insiden yang diusulkan pada lingkungan *cloud* yaitu melakukan pengumpulan file log dari aktivitas pengguna seperti log aplikasi, log *load balancer*, dan log *database* atau artefak digital untuk dilakukan proses analisis digital forensik (Ozer et al., 2020).

Paradigma proses digital forensik dan insiden respons dengan menggunakan pendekatan reaktif tidak relevan diterapkan pada lingkungan *cloud*. Diperlukan suatu pendekatan yang bersifat proaktif sehingga proses berjalan tanpa harus terjadi insiden

siber terlebih dahulu dalam artian diperlukan langkah monitoring dan deteksi secara proaktif. Dengan melakukan pendekatan proaktif maka hasil deteksi yang terindikasi anomali dapat dilakukan tindak lanjut berupa pengumpulan dan pengambilan barang bukti digital untuk proses analisis digital forensik. Proses digital forensik dan insiden respons bertujuan untuk mengumpulkan dan mendapatkan barang bukti digital yang relevan dengan insiden yang terjadi. Penggunaan lingkungan *cloud* memberikan tantangan ketika diperlukan proses pengambilan barang bukti digital karena pada lingkungan *cloud* tidak memungkinkan untuk dilakukan pengambilan barang bukti digital secara langsung. Pengambilan barang bukti digital pada lingkungan *cloud* lebih efektif dilakukan secara *remote* akses karena tidak diketahui di mana server berada (Machaka & Balan, 2022).

Sebagai langkah untuk menjawab tantangan dalam upaya pengumpulan dan pengambilan barang bukti digital serta upaya proaktif melakukan deteksi insiden, pada penelitian ini diusulkan penggunaan *tools opensource* untuk mengatasi hal tersebut. Tools yang diusulkan dalam penelitian ini yaitu Velociraptor dan Wazuh. Velociraptor merupakan salah satu platform *opensource* client-server yang digunakan untuk melakukan monitoring endpoint, digital forensic dan penanganan insiden. Aplikasi ini dikembangkan untuk mengumpulkan dan mengambil artefak pada perangkat endpoint seperti log aplikasi, log sistem, dan bahkan artefak malware atau malicious file (Rapid7, n.d.). Velociraptor disebutkan sebagai tools yang memiliki kemampuan paling baik dibandingkan dengan Cynet XDR dan GRR Rapid Response (Meyer et al., n.d.). Sedangkan Wazuh merupakan tools opensource yang dikembangkan oleh komunitas yang memiliki kemampuan sebagai Endpoint Detection and Response (XDR) dan Security Information and Event Management (SIEM). Wazuh dapat diterapkan dalam beberapa lingkungan seperti lingkungan local, lingkungan virtualisasi, docker dan kontainer, serta lingkungan berbasis *cloud* (Wazuh, 2023).

Pengujian sistem yang diusulkan dilakukan dengan melakukan serangan sesuai dengan konsep MITRE ATT&CK. MITRE ATT&CK merupakan kerangka kerja yang memberikan gambaran terkait dengan Taktik, Teknik, dan Prosedur (TTP) yang dilakukan oleh *threat actor* dalam melakukan suatu serangan siber (Machaka & Balan, 2022). Dengan mengikuti framework diharapkan Wazuh dapat mendeteksi serangan

yang terjadi sehingga dapat dilakukan aksi berupa pengambilan barang bukti digital dengan menggunakan Velociraptor. Skenario yang dijalankan dalam pengujian yaitu berupa aktivitas serangan untuk melakukan perubahan tampilan situs menjadi tampilan situs judi online (*web defacement* situs judi online) pada situs website di lingkungan *cloud*.

Berdasarkan latar belakang terkait dengan tantangan dalam proses pengumpulan dan pengambilan barang bukti digital serangan siber, penelitian ini mengusulkan penggunaan Velociraptor sebagai artefak *collection* dan Wazuh sebagai XDR dan SIEM yang diintegrasikan dengan Telegram untuk proses deteksi anomali.

1.2 Rumusan masalah

Berdasarkan latar belakang masalah yang telah dijelaskan, maka rumusan masalah pada penelitian yang dilakukan yaitu bagaimana implemantasi dan proses pengumpulan dan pengambilan barang bukti digital dengan menggunakan Velociraptor dan Wazuh.

1.3 Tujuan

Berdasarkan rumusan masalah yang telah ditentukan, tujuan dari penelitian yang dilakukan sebagai berikut:

1. Mampu melakukan integrasi antara Wazuh dan Telegram sebagai notifikasi dan penerapan Velociraptor dalam proses penanganan insiden.
2. Mampu melakukan rekonstruksi serangan *web defacement* situs judi online sesuai dengan *framework* Mitre Att&ck.
3. Mengukur keberhasilan implementasi Wazuh dan Velociraptor dalam melakukan deteksi dan respons terhadap insiden keamanan sebagai upaya preventif terhadap serangan *web defacement* situs judi online.
4. Mampu mengidentifikasi artefak digital pada lingkungan *cloud* menggunakan Velociraptor.

1.4 Manfaat

Adapun manfaat yang diharapkan dapat diperoleh dari penelitian yang dilakukan yaitu sebagai berikut:

1. Manfaat akademis

   Penelitian yang dilakukan diharapkan dapat memberikan pemahaman dan menambah pengetahuan terkait dengan implementasi Wazuh dan Velociraptor dalam konteks pengumpulan dan pengambilan artefak digital.

2. Manfaat non-akademis

   Penelitian yang dilakukan diharapkan dapat memberikan panduan praktis kepada organisasi atau profesional keamanan informasi dalam melakukan implementasi Wazuh dan Velociraptor untuk melakukan pengumpulan dan pengambilan artefak digital.

1.5 Batasan masalah

Adapun Batasan masalah dalam penelitian yang dilakukan antara lain:

1. Pengujian penggunaan Velociraptor dan Wazuh hanya dilakukan pada dua penyedia *cloud* yaitu Amazon *Cloud* Service dan Google *Cloud* Platform.
2. Pengujian serangan yang dilakukan yaitu berupa serangan *web defacement situs judi online* serta penyisipan *backdoor*.

1.6 Sistematika pembahasan

Dokumen penelitian ini terdiri dari 6 bagian dengan rincian sebagai berikut:

BAB I : PENDAHULUAN

: Bab 1 Pendahuluan, pada bagian ini membahas terkait dengan latar belakang, rumusan masalah, tujuan penelitian, Batasan penelitian, dan sistematika pembahasan.

BAB II : LANDASAN KEPUSTAKAAN

: Bab 2 Landasan Kepustakaan, pada bagian ini membahas terkait dengan konsep atau teori-teori dan literatur review pada penelitan terdahulu.

BAB III : METODOLOGI

: Bab 3 Metodologi, pada bagian ini membahas terkait dengan metode yang digunakan dalam melakukan penelitian

BAB IV : HASIL

: Bab 4 Hasil, pada bagian ini membahas terkait hasil penelitian yang diperoleh.

BAB V : PENUTUP

: Bab 5 Penutup, pada bagian ini membahas terkait kesimpulan dan saran dari penelitian yang dilakukan.