BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi telah memungkinkan organisasi untuk mengotomatisasi proses, memanfaatkan data secara lebih efektif, dan meningkatkan efisiensi operasional secara signifikan. Namun, seiring dengan meningkatnya ketergantungan terhadap infrastruktur digital, ancaman terhadap keamanan informasi juga berkembang secara drastis. Serangan siber kini tidak hanya bersifat acak, melainkan telah menjadi aktivitas yang terorganisir, sistematis, dan didukung oleh taktik serta teknik canggih yang sulit dideteksi oleh sistem keamanan tradisional. Akibatnya, organisasi menghadapi tekanan untuk terus mengevaluasi dan memperkuat pertahanan siber mereka.

Dalam upaya memperkuat ketahanan terhadap ancaman siber, simulasi serangan menjadi salah satu metode krusial untuk menguji kesiapan dan keandalan infrastruktur teknologi informasi. Salah satu alat yang cukup terkenal untuk simulasi pengujian dan analisis kerentanan adalah *Infection Monkey,* sebuah alat simulasi serangan yang efektif untuk mengidentifikasi kerentanan infrastruktur TI dengan meniru teknik aktor ancaman seperti eksploitasi jaringan, penyebaran lateral, dan eskalasi hak akses. Pada sebuah penelitian menunjukkan bahwa [1] *Infection Monkey* menempati posisi menengah dalam evaluasi alat emulasi serangan. Dengan skor 77.8% untuk instalasi dan 54.4% untuk *usability*, alat ini cukup mudah digunakan. Dukungan komunitas dan dokumentasi masing-masing mendapat 66.7% dan 61.9%, menunjukkan ketersediaan referensi yang baik. Namun, dalam hal *features & capabilities*, *Infection Monkey* hanya meraih 42.2%. Meskipun berada di posisi menengah, *Infection Monkey* sering kali menjadi pilihan utama untuk melakukan simulasi serangan, berkat kemampuannya yang teruji dalam mengidentifikasi kerentanannya serta kemudahan penggunaan yang membuatnya populer.

Pada penelitian [1] dengan judul "*Red Team Redemption: A Structured Comparison of Open-Source Tools for Adversary Emulation*" berfokus pada perbandingan terstruktur alat-alat *open-source* untuk emulasi ancaman (*adversary emulation*). Penelitian ini melakukan tinjauan komprehensif terhadap berbagai alat seperti *Infection Monkey*, *Caldera, Atomic Red Team*, dan lainnya. Perbandingan dilakukan dari segi fitur, kemampuan, dan kinerja masing-masing alat dalam meniru teknik, taktik, dan prosedur (TTP) yang digunakan oleh aktor ancaman.

Di sisi lain, penelitian kali ini akan menganalisis serangan menggunakan Infection Monkey pada sebuah organisasi dengan pendekatan MITRE ATT&CK dan CIS Controls untuk memahami taktik penyerang serta menyusun strategi mitigasi yang efektif. Hasil analisis menunjukkan bahwa rule dari sistem deteksi seperti Wazuh dan Elasticsearch belum sepenuhnya terhubung dengan framework MITRE ATT&CK, sehingga menghambat proses identifikasi teknik serangan. Sebagai solusi, penelitian ini mengembangkan rule khusus pada Wazuh agar setiap alarm dapat otomatis dipetakan ke taktik dan teknik MITRE ATT&CK, sehingga analisis insiden menjadi lebih cepat, akurat, dan kontekstual.

Kerangka kerja MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) merupakan basis pengetahuan yang lengkap yang mendokumentasikan taktik, teknik, dan prosedur (TTP) yang biasa digunakan oleh penyerang siber pada berbagai tahap serangan. Kerangka kerja ini memberikan pemahaman yang terstruktur dan rinci tentang cara ancaman siber beroperasi, sehingga menjadi sumber daya yang ampuh untuk meningkatkan strategi pertahanan keamanan siber [2].

Kerangka Kerja *MITRE ATT&CK* banyak diterapkan dalam berbagai penelitian maupun implementasi. Sebuah survei penelitian [3] menunjukkan bahwa lebih dari 80% perusahaan menggunakan *MITRE ATT&CK* untuk perlindungan terhadap ancaman. Selain itu, 57% dari peserta survei menyatakan bahwa mereka menggunakan *MITRE ATT&CK* untuk mengidentifikasi kesenjangan dalam solusi keamanan yang diterapkan di perusahaan mereka, sementara 55% merekomendasikannya untuk implementasi kebijakan keamanan dan 54% menggunakannya untuk pemodelan ancaman.

Selain itu, untuk meningkatkan efektivitas dalam melindungi sistem dari serangan, *CIS Controls* juga menjadi kerangka kerja yang penting dalam mendeteksi dan memitigasi ancaman. *CIS Controls* mengkategorikan dan memprioritaskan aktivitas keamanan siber berdasarkan kondisi organisasi. Kategorisasi ini dikenal sebagai CIS Implementation Groups (IGs). IGs adalah kategori yang dinilai sendiri oleh organisasi berdasarkan atribut keamanan siber yang ada[4].

1.2 Rumusan Masalah dan Solusi

Rumusan masalah yang dapat disimpulkan dari pembahasan sebelumnya adalah sebagai berikut:

1. Bagaimana kerentanan dalam infrastruktur TI dapat dieksploitasi melalui alat simulasi seperti *Infection Monkey*?

2. Apa dampak yang mungkin timbul dari penyalahgunaan *Infection Monkey* terhadap organisasi, khususnya dalam hal stabilitas sistem dan keamanan informasi?
3. Bagaimana integrasi metodo*log*i *MITRE ATT&CK* dan *CIS Controls* dapat membantu dalam memahami, menganalisis, dan memitigasi risiko serangan yang dilakukan menggunakan *Infection Monkey*?
4. Mengapa rule atau alarm yang dihasilkan oleh sistem deteksi seperti Wazuh belum secara otomatis terhubung dengan framework MITRE ATT&CK?
5. Bagaimana solusi pemetaan alarm ke framework MITRE ATT&CK dapat mempercepat dan meningkatkan efektivitas analisis insiden?

Maka dari itu, berikut beberapa solusi yang dapat dilakukan:

1. Melakukan analisis komprehensif terhadap serangan yang melibatkan *Infection Monkey* untuk memahami cara penyerang mengeksploitasi kerentanan.
2. Mengidentifikasi langkah-langkah mitigasi yang efektif untuk mencegah penyalahgunaan *Infection Monkey*, serta melindungi infrastruktur TI dari eksploitasi lebih lanjut.
3. Menerapkan metodo*log*i *MITRE ATT&CK* sebagai kerangka kerja untuk memahami tahapan serangan secara menyeluruh dan *CIS Controls* untuk prioritisasi langkah mitigasi yang relevan dan efektif.
4. Mengembangkan dan menerapkan rule khusus pada sistem deteksi (seperti Wazuh) agar alarm yang dihasilkan dapat otomatis terhubung dengan taktik dan teknik dalam framework MITRE ATT&CK.
5. Meningkatkan akurasi dan konteks analisis insiden melalui pemetaan otomatis ke framework MITRE ATT&CK.

Dengan demikian, analisis ini tidak hanya bertujuan untuk mengungkap dan memahami ancaman yang dapat ditimbulkan oleh penggunaan *Infection Monkey*, tetapi juga memberikan solusi dalam bentuk strategi mitigasi risiko yang dapat diterapkan.

1.3 Tujuan

Tujuan yang diharapkan dari kajian ini adalah sebagai berikut:

1. Mengidentifikasi secara menyeluruh potensi kerentanan yang dapat dieksploitasi melalui *Infection Monkey* dengan menggunakan analisis berbasis studi kasus.
2. Mengembangkan langkah mitigasi yang efektif dengan memanfaatkan metodo*log*i *MITRE ATT&CK* untuk analisis serangan dan *CIS Controls* sebagai panduan implementasi mitigasi.

3. Memberikan rekomendasi strategis bagi organisasi untuk meningkatkan kesadaran dan kemampuan dalam mendeteksi serta mengatasi serangan siber berbasis alat emulasi ancaman.
4. Meningkatkan efisiensi proses analisis insiden dengan menerapkan pemetaan otomatis alarm terhadap taktik dan teknik dalam MITRE ATT&CK menggunakan rule khusus pada Wazuh.
5. Membangun sistem monitoring yang mampu memberikan klasifikasi insiden secara real-time berdasarkan framework MITRE ATT&CK untuk mendukung pengambilan keputusan yang cepat dan tepat.

1.4 Penjadwalan Kerja

Selama menjalani kegiatan magang di PT Defender Nusa Semesta, penulis mengikuti jadwal masuk yang ditetapkan dari hari Minggu hingga Rabu setiap minggunya. Penugasan jam masuk magang diatur berdasarkan tiga shift: *early, middle*, dan *late*. Berikut adalah tabel jadwal magang untuk memudahkan pemahaman:

Tabel 1. 1 Jadwal kerja

NO	Shift	Hari			
		Minggu	Senin	Selasa	Rabu
1	Early	05.00 - 15.00			
2	Mid	10.00 - 20.00			
3	Late	19.30 – 05.30			

Dan berikut adalah jadwal guna untuk menyelesaikan Analisa serangan *Infection Monkey*: Timeline pengerjaan

Tabel 1. 2 Timeline pengerjaan

No	Deskripsi Kerja	Bulan				Bulan				Bulan				Bulan			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Analisa Awal																
2	Identifikasi kerentanan																
3	Analisis sistematis																
4	Penerapan kerangka kerja *MITRE ATT&CK*																
5	Penerapan *CIS Controls*																
6	Evaluasi																
7	Dokumentasi dan Publikasi																