Analisis Rantai Serangan dan Peningkatan Keamanan Berbasis Prinsip *Zero Trust* Menggunakan CISA *Zero Trust Maturity Model* (ZTMM): Studi Kasus *Post-mortem* pada Kompetisi *Attack-Defense* CTF KMIPN 2024

Vica Guneven[1], Maidel Fani[2]

* Politeknik Negeri Batam
Rekayasa Keamanan Siber
Jl. Ahmad Yani, Batam Centre, Batam 29461, Indonesia
E-mail: vicaadrn19@gmail.com
\# Politeknik Negeri Batam
Rekayasa Keamanan Siber
Jl. Ahmad Yani, Batam Centre, Batam 29461, Indonesia
E-mail: maidelfani@polibatam.ac.id

Abstrak

Penelitian ini menganalisis secara *post-mortem* rantai serangan 13 tahap pada mesin Amethysts dalam kompetisi *Attack-Defense* CTF KMIPN 2024 sebagai studi kasus pada lingkungan laboratorium. Setiap tahap dipetakan ke MITRE ATT&CK dan dianalisis menggunakan CVSS v3.1 untuk mengidentifikasi kerentanan serta menyusun kontrol keamanan berbasis prinsip *Zero Trust* menggunakan mekanisme keamanan bawaan Linux pada konfigurasi *Detect-First* dan *Full Enforcement*. Efektivitas kontrol diukur menggunakan *Attack Success Rate* (ASR), sedangkan tingkat kematangan kontrol dievaluasi menggunakan CISA *Zero Trust Maturity Model* (ZTMM) v2.0. Hasil menunjukkan ASR menurun dari 100% pada *baseline* menjadi 69,2% pada *Detect-First* dan 23,1% pada *Full Enforcement*. Evaluasi ZTMM menunjukkan peningkatan sejumlah fungsi menuju *tier Initial*, meskipun mayoritas fungsi masih berada pada *tier Traditional*. Temuan ini menunjukkan bahwa ASR dan ZTMM saling melengkapi dalam mengevaluasi efektivitas mitigasi serangan dan kematangan kontrol pada studi kasus lingkungan laboratorium, sehingga hasil penelitian ini tidak dimaksudkan untuk digeneralisasikan secara langsung pada lingkungan *enterprise*.

Kata kunci: *Zero Trust,* CISA ZTMM, *Attack chain, MITRE ATT&CK, CTF, Post-mortem Analysis*

Abstract

This study conducts a post-mortem analysis of a 13-stage attack chain on Amethysts machines in the KMIPN 2024 *Attack-Defense* CTF competition as a case study in a laboratory environment. Each stage was mapped to MITRE ATT&CK and analyzed using CVSS v3.1 to identify vulnerabilities and develop Zero Trust-based security controls using Linux's built-in security mechanisms in Detect-First and Full Enforcement configurations. Control effectiveness was measured using the Attack Success Rate (ASR), while control maturity was evaluated using the CISA Zero Trust Maturity Model (ZTMM) v2.0. The results showed that the ASR decreased from 100% in the baseline to 69.2% in the Detect-First configuration and 23.1% in the Full Enforcement configuration. The ZTMM evaluation revealed an improvement in several functions toward the Initial tier, although the majority of functions remained in the Traditional tier. These findings indicate that ASR and ZTMM complement each other in evaluating the effectiveness of attack mitigation and control maturity in a laboratory environment case study; therefore, the results of this study are not intended to be directly generalized to enterprise environments.

Keywords: *Zero Trust,* CISA ZTMM, *Attack chain,* MITRE ATT&CK, *CTF, Post-mortem Analysis*

1. Pendahuluan

Kompetisi Mahasiswa Informatika Politeknik Nasional (KMIPN) merupakan kompetisi tingkat nasional yang diselenggarakan oleh Politeknik Negeri se-Indonesia dan mencakup berbagai bidang, termasuk keamanan siber. Pelaksanaan kompetisi Keamanan Siber KMIPN 2024 menggunakan skema *Attack-Defense Capture The Flag* (CTF) yang mensimulasikan serangan pada lingkungan menyerupai kondisi nyata. Namun, fokus kompetisi lebih menitikberatkan pada keberhasilan

eksploitasi sistem, sedangkan analisis terhadap rantai serangan serta evaluasi penerapan kontrol pertahanan setelah serangan belum menjadi bagian dari kompetisi tersebut. Pada mesin Amethysts, rangkaian serangan menunjukkan bahwa sistem tanpa mekanisme pertahanan aktif masih rentan terhadap serangan berantai yang terstruktur. Berdasarkan lanskap keamanan siber Indonesia, berbagai serangan masih memanfaatkan kelemahan konfigurasi, layanan yang terbuka, dan kontrol keamanan yang tidak memadai [1]. Kondisi tersebut menunjukkan bahwa pendekatan keamanan tradisional berbasis perimeter belum mampu menghadapi ancaman *modern* yang bersifat multi-tahap dan adaptif.

Sebagai alternatif, konsep *Zero Trust Architecture* (ZTA) menekankan bahwa tidak ada entitas yang secara otomatis dipercaya, baik dari dalam maupun luar jaringan, sehingga seluruh akses harus diverifikasi secara berkelanjutan berdasarkan identitas, konteks, dan kebijakan keamanan yang berlaku [2]. Untuk mendukung implementasi dan evaluasi *Zero Trust*, CISA *Zero Trust Maturity Model* (ZTMM) v2.0 menyediakan kerangka kerja kematangan yang mencakup 5 pilar utama, yaitu Identity, Devices, Networks, Applications and Workloads, dan Data yang didukung oleh kapabilitas Cross-Cutting sebagai elemen lintas pilar [3].

Dalam konteks pendidikan keamanan siber, penelitian oleh Tirstan et al. menunjukkan bahwa kompetisi *Capture The Flag (*CTF) efektif untuk meningkatkan pengetahuan dan keterampilan peserta dalam menyelesaikan tantangan keamanan siber [4]. Namun, penelitian tersebut berfokus pada aspek pembelajaran dan performa peserta, tanpa melakukan analisis teknis terhadap rantai serangan yang terjadi maupun evaluasi peningkatan keamanan sistem setelah serangan berhasil dilakukan [4]. Penelitian lain oleh Fakhreja et al. menganalisis faktor-faktor yang memengaruhi tingkat keparahan insiden keamanan siber menggunakan pendekatan *machine learning* dan menghasilkan akurasi klasifikasi yang tinggi [5]. Meskipun demikian, penelitian tersebut tidak mengaitkan hasil analisis insiden dengan penerapan kontrol keamanan teknis maupun evaluasi tingkat kematangan keamanan berbasis kerangka kerja *Zero Trust* [5].

Dari sisi kematangan keamanan, Yeoh et al. mengusulkan kerangka penilaian kematangan *Zero Trust* untuk lingkungan pendidikan tinggi dan mengidentifikasi faktor-faktor keberhasilan implementasinya [6]. Namun, penelitian tersebut lebih menekankan aspek tata kelola dan manajemen organisasi serta belum divalidasi menggunakan data serangan teknis yang direkonstruksi dari skenario nyata [6]. Beberapa penelitian implementasi *Zero Trust* juga telah dilakukan pada lingkungan jaringan dan organisasi. Kusnanto et al. menunjukkan bahwa penerapan prinsip *Zero Trust* dapat meningkatkan keamanan jaringan melalui penguatan kontrol akses dan segmentasi jaringan [7]. Demikian pula, Rahman et al. menerapkan konsep *Zero Trust* pada arsitektur *enterprise* UMKM untuk meningkatkan keamanan akses terhadap sumber daya organisasi [8]. Akan tetapi, kedua penelitian tersebut berfokus pada implementasi arsitektur dan konfigurasi keamanan, tanpa mengukur efektivitas kontrol menggunakan *replay attack chain* maupun mengevaluasi dampaknya terhadap keberhasilan serangan secara kuantitatif [7], [8].

Berdasarkan kajian tersebut, terdapat tiga kesenjangan penelitian utama. Pertama, penelitian terkait CTF umumnya berfokus pada aspek pembelajaran peserta dan belum mengintegrasikan analisis teknis rantai serangan secara menyeluruh [4]. Kedua, penelitian *Zero Trust* yang ada lebih banyak berfokus pada tata kelola atau implementasi arsitektur tanpa validasi berbasis *replay attack chain* dan metrik keberhasilan serangan [6]–[8]. Ketiga, belum ditemukan penelitian yang menggabungkan analisis *post-mortem attack chain*, perancangan kontrol keamanan berbasis prinsip *Zero Trust*, serta evaluasi tingkat kematangan menggunakan *CISA Zero Trust Maturity Model (ZTMM) v2.0* dalam satu kerangka penelitian terpadu pada lingkungan *Attack-Defense CTF* [4], [6]–[8].

Berdasarkan uraian tersebut, permasalahan utama penelitian ini adalah bagaimana merancang kontrol keamanan berbasis prinsip *Zero Trust* yang mampu meningkatkan ketahanan sistem terhadap *attack chain* hasil rekonstruksi pada lingkungan *Attack-Defense* CTF, sekaligus mengevaluasi efektivitas kontrol tersebut terhadap keberhasilan serangan dan tingkat kematangan implementasinya menggunakan CISA *Zero Trust Maturity Model* (ZTMM).

Oleh karena itu, penelitian ini merekonstruksi dan menganalisis *post-mortem attack chain* pada mesin Amethysts KMIPN 2024, merancang dan mengimplementasikan kontrol keamanan berbasis prinsip *Zero Trust* menggunakan mekanisme keamanan bawaan Linux, kemudian mengevaluasi efektivitas kontrol melalui *Attack Success Rate* (ASR) serta tingkat kematangan menggunakan CISA *Zero Trust Maturity Model* (ZTMM) v2.0. Dengan demikian, penelitian ini tidak hanya menganalisis bagaimana serangan terjadi, tetapi juga mengukur secara empiris efektivitas kontrol keamanan yang diterapkan dalam mengurangi keberhasilan serangan dan meningkatkan tingkat kematangan keamanan sistem.

Berbeda dengan penelitian sebelumnya, penelitian ini memanfaatkan pengalaman pada kompetisi *Attack-Defense CTF* KMIPN 2024 sebagai dasar rekonstruksi *attack chain*. Lingkungan kompetisi tersebut menjadi studi kasus untuk merancang kontrol keamanan berbasis prinsip *Zero Trust*, kemudian mengevaluasi efektivitas mitigasi serangan menggunakan ASR serta mengevaluasi tingkat kematangan implementasi kontrol menggunakan *CISA Zero Trust Maturity Model*

(ZTMM). Dengan demikian, penelitian ini menghubungkan analisis serangan, implementasi kontrol keamanan, dan evaluasi kematangan dalam satu kerangka penelitian yang terpadu.

2. Landasan Teori

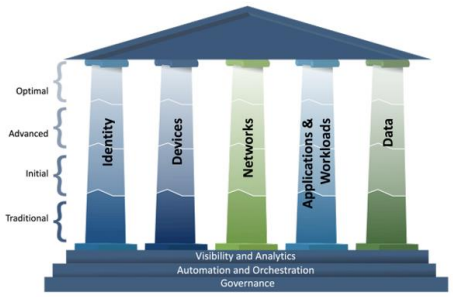
2.1 *Capture The Flag* dan *Attack chain*

Capture The Flag (CTF) merupakan metode pembelajaran keamanan siber berbasis simulasi yang memungkinkan peserta mengembangkan keterampilan identifikasi, eksploitasi, dan pertahanan sistem melalui lingkungan yang menyerupai kondisi serangan nyata [4]. Dalam penelitian ini, lingkungan *Attack-Defense* CTF KMIPN 2024 digunakan sebagai studi kasus untuk merekonstruksi *attack chain* yang berhasil mengompromikan mesin Amethysts. Setiap tahapan serangan kemudian dipetakan ke *framework* MITRE ATT&CK untuk mengidentifikasi teknik yang digunakan penyerang [10].

2.2 *Zero Trust Architecture*

Zero Trust Architecture (ZTA) merupakan pendekatan keamanan yang menghilangkan kepercayaan implisit terhadap pengguna maupun perangkat dengan menerapkan prinsip "*never trust, always verify dan least privilege access*." Setiap permintaan akses harus diverifikasi secara berkelanjutan berdasarkan identitas, perangkat, konteks, dan kebijakan keamanan yang berlaku [2]. Dalam penelitian ini, prinsip-prinsip *Zero Trust* digunakan sebagai acuan dalam perancangan kontrol keamanan yang kemudian dievaluasi menggunakan CISA *Zero Trust* Maturity Model.

2.3 CISA *Zero Trust Maturity Model* (ZTMM)



Gambar 1. Pilar *Zero Trust Maturity Model* (CISA, 2023)

CISA *Zero Trust Maturity Model* (ZTMM) merupakan kerangka evaluasi yang digunakan untuk mengukur tingkat kematangan implementasi *Zero Trust* berdasarkan lima pilar utama, yaitu Identity, Devices, Networks, Applications and Workloads, dan Data yang didukung oleh kapabilitas Cross-Cutting sebagai elemen lintas pilar [3]. Tingkat kematangan dibagi menjadi empat tahap, yaitu Traditional, Initial, Advanced, dan Optimal. Dalam penelitian ini, CISA ZTMM digunakan sebagai kerangka untuk mengevaluasi tingkat kematangan implementasi kontrol keamanan berbasis prinsip *Zero Trust* berdasarkan fungsi-fungsi yang didefinisikan pada setiap pilar sebelum dan sesudah penerapan kontrol.

2.4 *Post-mortem analysis*

Post-mortem analysis merupakan pendekatan analisis yang dilakukan setelah suatu insiden keamanan terjadi untuk memahami tahapan serangan, kerentanan yang dimanfaatkan, serta dampaknya terhadap sistem. Dalam penelitian ini, pendekatan tersebut digunakan untuk merekonstruksi *attack chain* berdasarkan *walkthrough* resmi mesin Amethysts dan menjadi dasar dalam perancangan kontrol keamanan serta evaluasi menggunakan CISA *Zero Trust* Maturity Model.

2.5 *Attack Success Rate* (ASR)

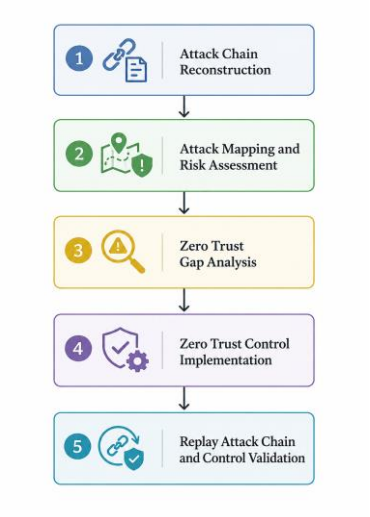
Attack Success Rate (ASR) digunakan dalam penelitian ini sebagai metrik evaluasi untuk mengukur efektivitas kontrol keamanan berdasarkan proporsi tahapan *attack chain* yang masih berhasil dieksekusi setelah implementasi kontrol. Nilai ASR dihitung sebagai perbandingan antara jumlah tahapan serangan yang berhasil (*successful stages*) dengan jumlah keseluruhan tahapan pada *attack chain* (*total stages*) dan dinyatakan dalam bentuk persentase.

Perhitungan ASR mengadopsi konsep proporsi (sample proportion) dalam statistika deskriptif, yaitu menyatakan perbandingan antara jumlah kejadian yang diamati dengan jumlah keseluruhan observasi dalam bentuk persentase sehingga memudahkan interpretasi hasil pengamatan [11]. Semakin rendah nilai ASR, semakin sedikit tahapan serangan yang berhasil direproduksi, sehingga menunjukkan bahwa kontrol keamanan yang diterapkan semakin efektif dalam membatasi progres *attack chain.* Nilai ASR pada penelitian ini merepresentasikan tingkat keberhasilan *replay attack* terhadap *attack chain* yang direkonstruksi dan tidak dimaksudkan untuk menggambarkan efektivitas kontrol terhadap seluruh kemungkinan variasi teknik serangan.

3. Metode Penelitian

Penelitian ini menggunakan metode studi kasus eksperimental dengan pendekatan *post-mortem attack*

chain analysis pada lingkungan laboratorium Amethysts yang digunakan dalam kompetisi *Attack-Defense* CTF KMIPN 2024. Metode penelitian terdiri dari lima tahapan utama, yaitu rekonstruksi *attack chain*, pemetaan serangan dan penilaian risiko, analisis kesenjangan *Zero Trust*, implementasi kontrol keamanan, serta *replay attack* dan evaluasi kontrol.



Gambar 2. Alur Metode Penelitian

3.1 Rekonstruksi *Attack chain*

Tahap pertama dilakukan dengan merekonstruksi rantai serangan berdasarkan *official walkthrough* mesin Amethysts pada kompetisi *Attack-Defense* CTF KMIPN 2024. Pendekatan *post-mortem analysis* digunakan untuk mengidentifikasi dan menyusun kembali urutan aktivitas yang dilakukan penyerang selama proses eksploitasi. Hasil rekonstruksi menghasilkan tiga belas tahapan serangan yang mencakup proses *reconnaissance*, enumerasi layanan, eksploitasi aplikasi web, *remote code execution*, akses jarak jauh melalui SSH, hingga *privilege escalation*. *Attack chain* yang berhasil direkonstruksi dan digunakan sebagai skenario dasar untuk analisis dan evaluasi keamanan pada tahap berikutnya.

3.2 Pemetaan Serangan dan Penilaian Risiko

Setelah *attack chain* direkonstruksi, setiap tahapan serangan dipetakan ke teknik yang sesuai pada *framework* MITRE ATT&CK untuk memperoleh representasi standar terhadap perilaku penyerang. Selanjutnya, kerentanan yang dimanfaatkan pada setiap tahapan dianalisis menggunakan *Common Vulnerability Scoring System* (CVSS) v3.1. Penilaian CVSS digunakan untuk menentukan tingkat keparahan kerentanan serta membantu dalam menentukan prioritas mitigasi yang menjadi dasar implementasi kontrol keamanan pada tahap berikutnya.

3.3 Analisis Kesenjangan *Zero Trust*

Analisis kesenjangan (*gap analysis*) dilakukan menggunakan CISA *Zero Trust Maturity Model* (ZTMM) versi 2.0. *Attack chain* yang telah direkonstruksi beserta kerentanan yang teridentifikasi dianalisis terhadap fungsi-fungsi kematangan yang terdapat pada pilar Identity, Devices, Networks, Applications and Workloads, dan Data dibarengi dengan Cross-Cutting Capabilities sebagai fungsi pendukung yang melintasi seluruh pilar. Hasil analisis digunakan untuk mengidentifikasi kelemahan keamanan pada setiap pilar ZTMM dan menjadi dasar evaluasi tingkat kematangan keamanan setelah implementasi kontrol.

3.4 Implementasi Kontrol Keamanan

Berdasarkan hasil analisis *attack chain*, pemetaan serangan menggunakan MITRE ATT&CK, penilaian risiko menggunakan CVSS v3.1, serta analisis kesenjangan terhadap CISA *Zero Trust Maturity Model* (ZTMM), dilakukan implementasi kontrol keamanan berbasis prinsip-prinsip *Zero Trust* menggunakan mekanisme keamanan bawaan Linux. Implementasi dilakukan pada dua konfigurasi lingkungan pengujian, yaitu VM2 (*Detect-First*) dan VM3 (*Full Enforcement*).

VM2 merepresentasikan pendekatan *Detect-First* yang berfokus pada peningkatan visibilitas melalui mekanisme *monitoring*, logging, dan deteksi aktivitas serangan dengan tetap mempertahankan ketersediaan layanan. Sementara itu, VM3 merepresentasikan pendekatan *Full Enforcement* dengan menerapkan kontrol keamanan tambahan untuk membatasi dan mencegah aktivitas berbahaya secara aktif.

Kontrol yang diterapkan meliputi pembatasan akses layanan, monitoring aktivitas sistem, proteksi aplikasi, penguatan konfigurasi layanan (*service hardening*), perlindungan data, serta penghapusan kapabilitas sistem yang berisiko. Selanjutnya, kontrol-kontrol tersebut dipetakan terhadap pilar CISA *Zero Trust Maturity Model* (ZTMM) sebagai dasar evaluasi tingkat kematangan keamanan setelah implementasi.

3.5 *Replay attack* dan Evaluasi Kontrol

Untuk mengevaluasi efektivitas kontrol keamanan yang diterapkan, *attack chain* yang telah direkonstruksi diulang (*replay attack*) pada setiap lingkungan pengujian menggunakan prosedur dan perintah serangan yang sama. *Replay attack* dilakukan untuk mengidentifikasi tahapan serangan yang masih berhasil dieksekusi setelah

implementasi kontrol keamanan.

Replay attack dilakukan menggunakan urutan tahapan, teknik, dan prosedur serangan yang sama dengan hasil rekonstruksi *attack chain*. Oleh karena itu, evaluasi ini mengukur efektivitas kontrol terhadap skenario serangan yang direproduksi, bukan terhadap variasi teknik serangan baru maupun ancaman yang berbeda.

Selain itu, dilakukan proses validasi kontrol untuk memastikan bahwa kegagalan suatu tahapan serangan benar-benar disebabkan oleh kontrol keamanan yang diterapkan, bukan oleh faktor eksternal lainnya. Setiap kontrol diuji melalui skenario validasi tersendiri untuk memastikan fungsi mitigasinya berjalan sesuai tujuan.

Efektivitas kontrol keamanan kemudian dievaluasi menggunakan *Attack Success Rate* (ASR). Pada penelitian ini, ASR dihitung sebagai proporsi tahapan serangan yang masih berhasil direproduksi *(successful stages)* terhadap jumlah keseluruhan tahapan pada *attack chain (total stages)*, kemudian dinyatakan dalam bentuk persentase sesuai konsep proporsi pada statistika deskriptif [11].

$$ASR = \frac{Successful\ Stages}{Total\ Stages} \times 100\%$$

Keterangan:

- *Successful stages*: jumlah tahapan serangan yang berhasil dieksekusi.
- *Total stages*: jumlah keseluruhan tahapan pada *attack chain*.

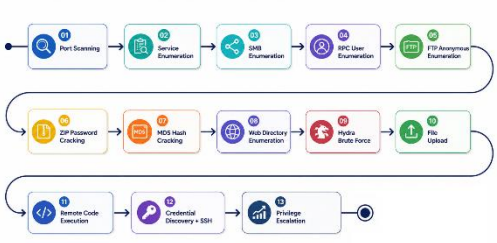
Semakin rendah nilai ASR, semakin sedikit tahapan serangan yang berhasil direproduksi, sehingga menunjukkan bahwa kontrol keamanan semakin efektif dalam membatasi progres serangan pada skenario yang diuji.

Selain ASR, penelitian ini juga menggunakan CISA *Zero Trust Maturity Model* (ZTMM) untuk mengevaluasi tingkat kematangan implementasi kontrol berbasis prinsip *Zero Trust*. Evaluasi dilakukan dengan memetakan kontrol keamanan yang diterapkan terhadap fungsi-fungsi pada setiap pilar ZTMM. Dengan demikian, ASR digunakan untuk mengukur efektivitas kontrol dalam membatasi keberhasilan *attack chain*, sedangkan ZTMM digunakan untuk mengevaluasi tingkat kematangan implementasi kontrol. Kedua metrik tersebut saling melengkapi karena mengevaluasi aspek keamanan yang berbeda.

4. Hasil dan Pembahasan

4.1 Rekonstruksi *Attack chain*

Analisis *post-mortem* dilakukan terhadap *walkthrough* Amethysts untuk merekonstruksi urutan aktivitas serangan yang dilakukan oleh penyerang. Proses rekonstruksi digunakan untuk mengidentifikasi jalur serangan, kerentanan yang dieksploitasi, serta hubungan antar tahapan serangan. *Attack chain* yang dihasilkan digunakan sebagai skenario dasar untuk penilaian kerentanan, analisis kesenjangan *Zero Trust*, dan evaluasi kontrol keamanan.



Gambar 3. Rekonstruksi *Attack chain* Mesin Amethysts

Gambar 3 menunjukkan alur serangan yang direkonstruksi berdasarkan *walkthrough*. Serangan diawali dengan aktivitas *discovery* dan *enumeration* layanan, kemudian dilanjutkan dengan perolehan kredensial melalui layanan yang terekspos dan mekanisme autentikasi yang lemah. Selanjutnya penyerang memperoleh akses ke aplikasi web, mengunggah *web shell* berbahaya, mengeksekusi perintah jarak jauh, memperoleh kredensial tambahan, dan akhirnya mendapatkan hak akses root pada sistem target.

Tabel I. Hasil Rekonstruksi *Attack chain* Amethysts

No	Tahapan	Tool	Output
1	*Port scanning*	nmap -p-	Ditemukan 6 port terbuka: 21, 22, 80, 81, 1139, 1445
2	*Service enumeration*	nmap -sCV	Versi layanan dan banner berhasil diidentifikasi
3	*SMB Enumeration*	smbclient	Ditemukan share backup yang dapat diakses
4	*RPC User Enumerati*	rpcclient (null	Diperoleh 9 username sistem

	on	session)	
5	*FTP Anonymous Enumeration*	wget -r	backup.zip berhasil diunduh
6	*ZIP Password Cracking*	zip2john + john	Password ZIP (pinkgirl) berhasil diperoleh
7	*MD5 Hash Cracking*	crackstation	Diperoleh 4 password plaintext
8	*Web Directory enumeration*	gobuster	Ditemukan direktori /prospective (RiteCMS 3.0)
9	*Hydra Brute force*	hydra http-post-form	Kredensial valid berhasil ditemukan
10	*File upload*	RiteCMS file manager	shell.php berhasil diunggah ke direktori web
11	*Remote code execution*	Akses langsung ke shell.php	Eksekusi perintah berhasil dilakukan dengan hak akses web server
12	*Credential discovery + Remote Access*	cat .env + SSH	Akses sebagai pengguna jossie dan perolehan user flag
13	*Privilege escalation*	*Linux capability* abuse (cap_setuid)	Hak akses administratif dan root flag berhasil diperoleh

Proses rekonstruksi berhasil mengidentifikasi tiga belas tahapan serangan yang mencakup fase *discovery*, *credential access*, eksploitasi aplikasi, dan *privilege escalation*. Tahapan tersebut selanjutnya dipetakan ke MITRE ATT&CK dan dievaluasi menggunakan CVSS untuk mendukung perancangan serta implementasi kontrol keamanan yang dirancang berdasarkan prinsip-prinsip *Zero Trust*.

4.2 Penilaian Kerentanan dan Analisis Gap *Zero Trust*

Attack chain yang telah direkonstruksi dianalisis untuk mengidentifikasi kerentanan yang dieksploitasi pada setiap tahapan serangan. Untuk menstandarkan proses analisis, seluruh tiga belas tahapan dipetakan ke kerangka kerja MITRE ATT&CK. Namun demikian, hanya tahapan yang berkaitan langsung dengan kelemahan keamanan yang dieksploitasi yang dimasukkan ke dalam penilaian CVSS dan analisis gap *Zero Trust*. Aktivitas *discovery* dan *enumeration*, seperti pemindaian port *(port scanning)*, enumerasi layanan (*service enumeration)*, serta enumerasi direktori *(directory enumeration)*, tidak dimasukkan karena merepresentasikan perilaku penyerang, bukan kerentanan pada sistem target.

Meskipun *attack chain* terdiri dari tiga belas tahapan, hanya delapan tahapan yang dimasukkan dalam penilaian kerentanan. *Port scanning* (T1046), *service enumeration* (T1046), ZIP *password cracking* (T1110.002), MD5 *hash cracking* (T1110.002), dan *web directory enumeration* (T1083) dikecualikan karena aktivitas tersebut merupakan teknik yang digunakan penyerang atau tindakan pasca-kompromi, bukan kelemahan inheren pada lingkungan target. Oleh karena itu, penilaian CVSS difokuskan pada kelemahan yang secara langsung memungkinkan akses tidak sah, kompromi kredensial, *remote code execution*, dan *privilege escalation*.

Kerentanan yang teridentifikasi kemudian dinilai menggunakan Common Vulnerability Scoring System (CVSS) untuk menentukan tingkat keparahan dan prioritas mitigasi. Selanjutnya, setiap kerentanan dipetakan ke pilar yang sesuai dalam CISA *Zero Trust Maturity Model* (ZTMM) untuk mengidentifikasi kesenjangan keamanan pada setiap domain *Zero Trust*. Hasil analisis kesenjangan tersebut digunakan sebagai acuan dalam mengevaluasi keterkaitan kontrol keamanan yang diterapkan terhadap masing-masing pilar ZTMM.

Tabel II. Penilaian Kerentanan dan Analisis Gap *Zero Trust*

Tahapan Serangan	**Teknik MITRE ATT&CK**	**CVSS**	**Pilar ZTMM**
SMB *Enumeration*	T1135 – Network Share Discovery	5.3	Networks
RPC *User Enumeration*	T1087.001 – Account Discovery : Local Account	5.3	Networks

FTP *Anonymous Enumeration*	T1078.001 – Valid Accounts: Default Accounts	7.5	Networks
Hydra Brute force	T1110.001 – Password Guessing	6.5	Identity
File upload	T1505.003 – Server Software Component: Web shell	9.9	Applications and Workloads
Remote code execution	T1190 – Exploit Public-Facing Application	10.0	Applications and Workloads
Credential discovery + Remote Access	T1552.001 – Unsecured Credentials: Credentials In Files T1021.004 – Remote Services: SSH	7.7	Data
Privilege escalation	T1548.001 – Abuse Elevation Control Mechanism: Setuid and Setgid	7.8	Devices

Sebagaimana ditunjukkan pada Tabel II, kerentanan dengan tingkat risiko tertinggi berada pada lapisan aplikasi, khususnya *unrestricted file upload* (T1505.003, CVSS 9.9) dan *remote code execution* (T1190, CVSS 10.0). Kerentanan tersebut memungkinkan penyerang memperoleh akses tidak sah dan mengeksekusi perintah arbitrer pada sistem target sehingga menjadi fokus utama dalam perancangan kontrol *Zero Trust*.

Penilaian juga mengidentifikasi kerentanan terkait paparan kredensial dan *privilege escalation* sebagai faktor penting yang memungkinkan penyerang mencapai kompromi sistem secara penuh. Sebelum implementasi kontrol *Zero Trust*, fungsi keamanan yang terdampak dikategorikan pada tahap Traditional berdasarkan CISA *Zero Trust Maturity Model*, yang menunjukkan keterbatasan pada aspek *Enforcement*, visibility, dan automated *monitoring*. Oleh karena itu, kesenjangan yang teridentifikasi menjadi dasar dalam perancangan dan implementasi kontrol *Zero Trust* pada lingkungan eksperimen.

4.3 Implementasi Kontrol Keamanan

Berdasarkan hasil analisis *attack chain*, pemetaan serangan menggunakan MITRE ATT&CK, penilaian risiko menggunakan CVSS v3.1, serta analisis kesenjangan terhadap CISA *Zero Trust Maturity Model* (ZTMM), dilakukan implementasi kontrol keamanan berbasis prinsip *Zero Trust* pada dua lingkungan eksperimen, yaitu VM2 (*Detect-First*) dan VM3 (*Full Enforcement*). Implementasi kontrol difokuskan pada mitigasi kerentanan yang teridentifikasi selama proses rekonstruksi *attack chain* untuk meningkatkan efektivitas pertahanan terhadap skenario serangan yang diuji.

VM2 dirancang dengan pendekatan *Detect-First*, yang berfokus pada peningkatan visibilitas melalui mekanisme monitoring, logging, dan alerting tanpa mengurangi ketersediaan layanan secara signifikan. Sementara itu, VM3 menerapkan pendekatan *Full Enforcement* dengan kontrol keamanan yang lebih ketat untuk membatasi atau mencegah aktivitas penyerang secara langsung.

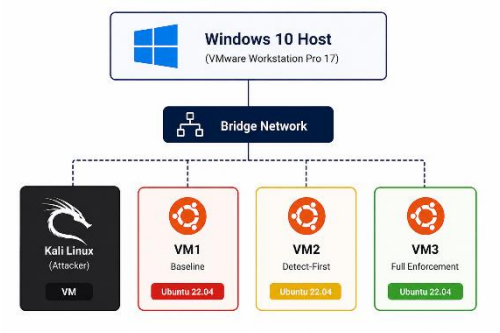
Setelah seluruh kontrol diterapkan, setiap kontrol dipetakan terhadap pilar-pilar CISA *Zero Trust Maturity Model* (ZTMM) untuk menunjukkan hubungan antara kelemahan yang diidentifikasi, kontrol keamanan yang diterapkan, dan domain *Zero Trust* yang dievaluasi. Hasil pemetaan implementasi kontrol terhadap setiap pilar ZTMM ditunjukkan pada Tabel III.

Tabel III. Implementasi Kontrol Keamanan

Pilar ZTMM	**Gap Analisis**	**VM2**	**VM3**
Identity	Tidak ada pembatasan autentikasi dan *brute force*	Fail2ban (SSH & HTTP jail), SSH MaxAuthTries	Fail2ban (threshold lebih ketat), AllowUsers, PasswordAuthentication disabled, pembatasan sesi SSH
Devices	Monitoring sistem dan perlindungan *host*	auditd monitoring, audit rules	auditd monitoring, audit rules, penghapusan

	terbatas		*Linux capability*
Networks	SMB dan FTP dapat diakses tanpa pembatasan	nftables micro-perimeter, ZT-SMB rule, ZT-FTP rule, egress monitoring	nftables, Samba restrict anonymous, FTP anonymous disable
Application and Workloads	Upload file dan eksekusi kode tidak terkontrol	Upload monitoring (inotify), nginx access logging, admin activity logging	inotify monitoring, nginx logging, PHP disable_functions
Data	Kredensial disimpan dalam plaintext dan tidak terinventarisasi	Permission `.env` (640), owner root:www-data	Enkripsi `.env.enc`, xattr sensitivity label, data inventory
Cross-Cutting Capabilities	Logging dan validasi kebijakan belum terpusat	ZT centralized logging, FTP monitoring, policy manifest, *compliance* checker	ZT centralized logging, FTP monitoring (inherited), policy manifest & Compliance Checker (diperluas)

Kontrol keamanan berbasis prinsip *Zero Trust* yang telah diterapkan kemudian dipetakan terhadap pilar-pilar CISA *Zero Trust Maturity Model* (ZTMM), yaitu Identity, Devices, Networks, Applications and Workloads, Data, serta Cross-Cutting Capabilities sebagai fungsi pendukung yang melintasi seluruh pilar. Pemetaan ini bertujuan untuk menunjukkan keterkaitan antara kontrol yang diimplementasikan dengan domain *Zero Trust* yang relevan, serta menjadi dasar dalam proses evaluasi tingkat kematangan pada tahap berikutnya. VM2 menekankan peningkatan visibilitas melalui mekanisme monitoring, logging, dan deteksi insiden, sedangkan VM3 mengombinasikan kemampuan tersebut dengan kontrol preventif yang lebih ketat untuk membatasi peluang keberhasilan serangan.



Gambar 4. Arsitektur Kontrol *Zero Trust*

Gambar 4 menggambarkan arsitektur lingkungan eksperimen yang digunakan dalam penelitian. VM1 merepresentasikan lingkungan dasar (*baseline*) tanpa kontrol keamanan tambahan. VM2 menerapkan pendekatan *Detect-First* dengan menambahkan mekanisme monitoring, logging, dan deteksi aktivitas sistem, sedangkan VM3 menerapkan pendekatan *Full Enforcement* melalui penambahan kontrol preventif untuk membatasi aktivitas penyerang secara langsung. Arsitektur ini memungkinkan *replay attack* dilakukan pada setiap lingkungan secara konsisten sehingga efektivitas kontrol keamanan dapat dibandingkan menggunakan metrik *Attack Success Rate* (ASR) dan dievaluasi terhadap CISA *Zero Trust Maturity Model* (ZTMM).

4.4 Hasil *Replay attack chain*

Untuk mengevaluasi efektivitas kontrol keamanan yang telah diterapkan, rantai serangan 13 tahap yang direkonstruksi dijalankan ulang (*replay attack*) pada seluruh lingkungan eksperimen menggunakan prosedur, urutan tahapan, dan teknik serangan yang sama seperti pada skenario hasil rekonstruksi. *Replay attack* dilakukan untuk mengidentifikasi tahapan serangan yang masih berhasil dieksekusi setelah implementasi kontrol keamanan. Dengan demikian, pengujian pada penelitian ini mengevaluasi kemampuan kontrol dalam memitigasi *attack chain* yang sama, bukan variasi teknik serangan baru. Hasil *replay attack* pada setiap tahapan ditunjukkan pada Tabel IV.

Tabel IV. Hasil *Replay attack chain* pada Setiap Lingkungan Pengujian

No	Tahapan Serangan	VM1	VM2	VM3
1	*Port scanning*	✓	✓	✓
2	*Service enumeration*	✓	✓	✓

3	SMB *Enumeration*	✓	✓	✗
4	RPC User *Enumeration*	✓	✓	✗
5	FTP Anonymous *Enumeration*	✓	✓	✗
6	ZIP Password Cracking	✓	✓	✗
7	MD5 Hash Cracking	✓	✓	✗
8	Web *Directory enumeration*	✓	✓	✓
9	Hydra *Brute force*	✓	✓	✗
10	*File upload*	✓	✗	✗
11	*Remote code execution*	✓	✗	✗
12	*Credential discovery* + SSH Access	✓	✗	✗
13	*Privilege escalation*	✓	✗	✗

Berdasarkan hasil *replay attack* pada Tabel IV, jumlah tahapan serangan yang berhasil dieksekusi pada setiap lingkungan kemudian dihitung menggunakan metrik *Attack Success Rate* (ASR).

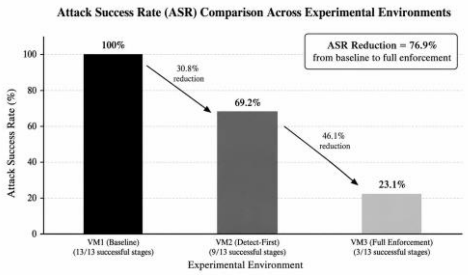
Tabel V. Hasil *Replay attack chain*

Environment	***Successful stages***	***Total stages***	**ASR**
VM1 (*Baseline*)	13	13	100.0%
VM2 (*Detect-First*)	9	13	69.2%
VM3 (*Full Enforcement*)	3	13	23.1%

Sebagaimana ditunjukkan pada Tabel V, seluruh tahapan serangan berhasil dieksekusi pada VM1, sehingga menghasilkan ASR sebesar 100%. Hasil ini mengonfirmasi bahwa rantai serangan yang direkonstruksi dapat direproduksi sepenuhnya pada lingkungan *baseline* dan oleh karena itu menyediakan titik referensi yang valid untuk mengevaluasi efektivitas kontrol keamanan yang diterapkan.

VM2 menurunkan ASR menjadi 69,2% dengan tetap mempertahankan ketersediaan layanan inti. Mekanisme monitoring dan logging yang diterapkan meningkatkan visibilitas terhadap aktivitas penyerang tanpa secara langsung membatasi seluruh tahapan serangan. Mekanisme pemantauan seperti fail2ban, auditd, inotify, dan *centralized logging* berhasil merekam aktivitas penyerang selama tahapan awal rantai serangan. Selain itu, perlindungan unggah berbasis inotify secara otomatis mendeteksi dan mengganti nama file *web shell* yang diunggah, sehingga mencegah keberhasilan *deployment payload* berbahaya. Akibatnya, rantai serangan terhenti pada tahap unggah file, dan tahapan selanjutnya berupa *remote code execution*, *credential access*, serta *privilege escalation* tidak dapat dilakukan.

Peningkatan paling signifikan diamati pada VM3, di mana ASR menurun menjadi 23,1%. Kontrol yang berorientasi pada *Enforcement*, termasuk *service hardening*, autentikasi SSH berbasis *public key*, penghapusan *Linux capability*, dan pembatasan akses yang lebih ketat, mencegah penyerang untuk melanjutkan serangan melampaui tahap awal *reconnaissance* dan *enumeration*. Sebagai hasilnya, aktivitas *credential access*, akses jarak jauh berbasis SSH, *deployment web shell*, *remote code execution*, dan *privilege escalation* berhasil dimitigasi secara efektif.



Gambar 5. Perbandingan *Attack Success Rate* (ASR) pada Berbagai Lingkungan Eksperimen

Gambar 5 memvisualisasikan penurunan ASR secara bertahap pada ketiga lingkungan pengujian. Jumlah tahapan serangan yang berhasil menurun dari 13 pada VM1 menjadi 9 pada VM2 dan selanjutnya menjadi 3 pada VM3. Hasil ini menunjukkan bahwa implementasi kontrol keamanan secara bertahap dan signifikan mengurangi keberhasilan serangan serta membatasi progresi penyerang di sepanjang rantai serangan yang direkonstruksi.

Perlu dicatat bahwa nilai ASR pada penelitian ini diperoleh dari *replay attack* terhadap *attack chain* yang sama pada seluruh lingkungan pengujian. Oleh karena itu, hasil ASR merepresentasikan efektivitas kontrol

keamanan dalam memitigasi skenario serangan yang direkonstruksi, sedangkan evaluasi terhadap variasi teknik serangan lain berada di luar ruang lingkup penelitian ini.

4.5 Evaluasi Kematangan *Zero Trust*

Berdasarkan CISA *Zero Trust Maturity Model* (ZTMM) v2.0 [3], tingkat kematangan implementasi *Zero Trust* diklasifikasikan ke dalam empat tahap, yaitu Traditional (T), Initial (I), Advanced (A), dan Optimal (O). Tahap Traditional umumnya masih bergantung pada konfigurasi keamanan manual, kebijakan yang bersifat statis, mekanisme enforcement yang terisolasi, serta visibilitas yang terbatas. Tahap Initial mulai memperkenalkan otomatisasi dasar, *policy enforcement*, dan visibilitas yang teragregasi. Tahap Advanced ditandai dengan integrasi antarpilar, otomatisasi yang lebih luas, serta pengambilan keputusan keamanan berbasis risiko (*risk-adaptive*). Sementara itu, tahap Optimal merepresentasikan implementasi *Zero Trust* yang telah menerapkan *continuous verification*, orkestrasi keamanan yang terintegrasi, serta kebijakan yang dinamis dan adaptif di seluruh lingkungan. Evaluasi pada penelitian ini dilakukan secara literal terhadap fungsi-fungsi yang didefinisikan pada CISA ZTMM v2.0, sehingga setiap fungsi dinilai berdasarkan bukti konfigurasi aktual, bukan berdasarkan keberadaan suatu perangkat lunak atau tool keamanan.

Mengingat penelitian ini dilakukan pada lingkungan laboratorium berbasis satu mesin (*single-host laboratory environment*) menggunakan mekanisme keamanan bawaan Linux, evaluasi difokuskan pada pemenuhan fungsi-fungsi ZTMM yang dapat dibuktikan melalui konfigurasi aktual. Kapabilitas yang mensyaratkan infrastruktur organisasi yang lebih luas, seperti orkestrasi lintas sistem, *risk-adaptive* policy engine, *continuous verification*, maupun integrasi identitas tingkat *enterprise*, berada di luar ruang lingkup penelitian ini.

Sebanyak 40 fungsi dievaluasi, terdiri atas 7 fungsi pada pilar Identity, 7 fungsi pada Devices, 7 fungsi pada Networks, 8 fungsi pada Applications and Workloads, 8 fungsi pada Data, serta 3 fungsi pada kapabilitas Cross-Cutting. Penentuan *Overall Stage* setiap pilar menggunakan metode agregasi *majority* (modus), yaitu *tier* yang dicapai oleh mayoritas fungsi dalam suatu pilar digunakan sebagai representasi tingkat kematangan pilar tersebut.

Tabel VI. Evaluasi Kematangan ZTMM Secara Keseluruhan

Pillar	**VM1**	**VM2**	**VM3**
Identity	*Traditional (T)*	*T*	*T*
Devices	*T*	*T*	*T*
Networks	*T*	*T*	*T*
Applications and Workloads	*T*	*T*	*T*
Data	*T*	*T*	*T*
Overall	**Traditional**		
Cross-Cutting Capabilities	*T*	*Initial (I)*	*Initial (I)*

Sebelum implementasi kontrol keamanan, seluruh 40 fungsi pada VM1 berada pada tahap Traditional, menunjukkan bahwa lingkungan masih mengandalkan hubungan kepercayaan implisit (*implicit trust*) tanpa dukungan *visibility*, *automated monitoring*, maupun *policy enforcement* yang memadai.

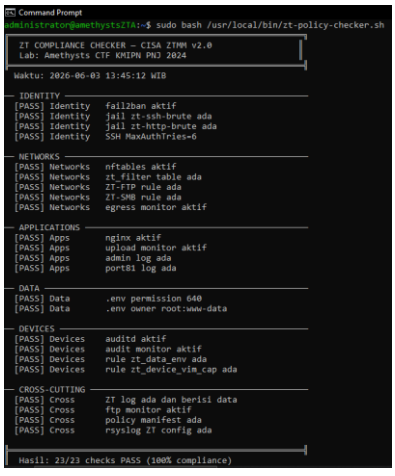
Setelah implementasi kontrol keamanan, jumlah fungsi yang mencapai tahap Initial meningkat menjadi 7 fungsi (17,5%) pada VM2 dan 12 fungsi (30%) pada VM3. Meskipun demikian, peningkatan tersebut belum mengubah *Overall Stage* pada lima pilar utama (Identity, Devices, Networks, Applications and Workloads, dan Data) karena sebagian besar fungsi pada masing-masing pilar masih berada pada tahap Traditional berdasarkan kriteria literal CISA ZTMM. Peningkatan tingkat kematangan hanya terjadi pada kapabilitas Cross-Cutting, di mana dua dari tiga fungsi berhasil mencapai tahap Initial, sehingga *Overall Stage* kapabilitas tersebut meningkat dari Traditional menjadi Initial.

Walaupun *Overall Stage* sebagian besar pilar tidak berubah, evaluasi pada tingkat fungsi menunjukkan adanya peningkatan kapabilitas keamanan. Pada pilar Identity, peningkatan terjadi pada fungsi *Risk Assessment* melalui konfigurasi Fail2ban yang lebih ketat pada VM3 sehingga serangan *brute force* dapat dihentikan lebih awal dibandingkan VM2. Pada pilar Networks dan Devices, penerapan nftables serta auditd meningkatkan fungsi *Visibility and analytics*, sedangkan pada pilar Data, VM3 berhasil meningkatkan empat fungsi melalui inventarisasi data, pelabelan sensitivitas menggunakan extended attributes (xattr), serta implementasi mekanisme

enkripsi. Namun demikian, beberapa fungsi seperti Traffic Encryption, Device Threat Protection, dan Secure Application Development tetap berada pada tahap Traditional karena memerlukan infrastruktur tambahan yang berada di luar ruang lingkup penelitian ini.

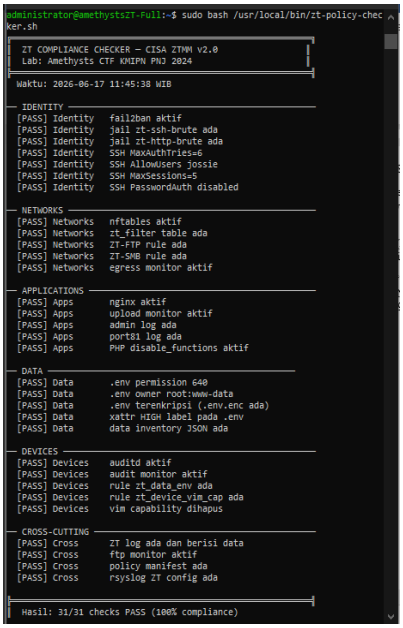
Perbedaan kedalaman implementasi kontrol tersebut tercermin pada hasil *replay attack chain.* Meskipun VM2 dan VM3 memiliki *Overall Stage* yang sama pada sebagian besar pilar, yaitu Traditional, keduanya menunjukkan efektivitas mitigasi yang berbeda. VM2 menghasilkan *Attack Success Rate* (ASR) sebesar 69,2%, sedangkan VM3 berhasil menurunkannya menjadi 23,1%. Temuan ini menunjukkan bahwa *Attack Success Rate* dan ZTMM mengevaluasi aspek keamanan yang berbeda. ASR mengukur efektivitas kontrol dalam menghentikan rantai serangan yang diuji, sedangkan ZTMM mengevaluasi kelengkapan implementasi kapabilitas *Zero Trust* berdasarkan fungsi-fungsi yang didefinisikan CISA. Oleh karena itu, dua lingkungan dengan *Overall Stage* yang sama dapat memiliki tingkat ketahanan terhadap serangan yang berbeda apabila kedalaman implementasi kontrol pada tingkat fungsi tidak sama.

Untuk memastikan bahwa seluruh kontrol keamanan yang menjadi dasar evaluasi telah diterapkan sesuai rancangan penelitian, dilakukan proses validasi menggunakan *Zero Trust* Compliance Checker yang dikembangkan secara khusus.



Gambar 6. Hasil Validasi Kepatuhan *Zero Trust*

Hasil pengujian pada VM2 menunjukkan bahwa seluruh 23 pemeriksaan kebijakan berhasil dipenuhi (23/23 atau 100% *compliance*).



Gambar 7. Hasil Validasi Kepatuhan *Zero Trust* VM3

Hasil pengujian pada VM3 juga menunjukkan bahwa seluruh 31 pemeriksaan kebijakan berhasil dipenuhi (31/31 atau 100% *compliance*).

Compliance Checker tidak digunakan untuk menentukan *tier* ZTMM maupun mengukur efektivitas pertahanan terhadap serangan secara langsung. Pengujian ini hanya memverifikasi bahwa seluruh kontrol keamanan yang dirancang dalam penelitian telah diterapkan sesuai konfigurasi yang ditetapkan pada policy.json sebelum dilakukan evaluasi menggunakan *replay attack* dan CISA ZTMM. Dengan demikian, capaian 100% *compliance* menunjukkan bahwa konfigurasi sistem telah sesuai dengan rancangan kontrol yang ditetapkan, **namun tidak secara otomatis** menunjukkan bahwa implementasi *Zero Trust* telah mencapai tingkat kematangan tertentu ataupun memberikan perlindungan yang optimal terhadap seluruh jenis serangan.

Secara keseluruhan, implementasi kontrol keamanan berhasil meningkatkan ketahanan sistem terhadap *attack chain* yang direkonstruksi sebagaimana ditunjukkan oleh penurunan *Attack Success Rate* pada VM2 dan VM3. Namun, evaluasi menggunakan CISA *Zero Trust Maturity Model* menunjukkan bahwa sebagian besar fungsi masih berada pada tahap Traditional, karena banyak kapabilitas *Zero Trust* yang dipersyaratkan untuk mencapai *tier* yang lebih tinggi belum diterapkan pada lingkungan laboratorium ini. Temuan ini menunjukkan

bahwa peningkatan efektivitas mitigasi terhadap serangan tidak selalu diikuti oleh peningkatan tingkat kematangan ZTMM, karena kedua metrik tersebut mengevaluasi aspek keamanan yang berbeda dan saling melengkapi.

4.6 Pembahasan

Hasil penelitian menunjukkan bahwa implementasi kontrol keamanan yang dirancang berdasarkan hasil analisis *attack chain*, kemudian dievaluasi menggunakan CISA *Zero Trust Maturity Model* (ZTMM), mampu menurunkan tingkat keberhasilan rantai serangan secara signifikan. Berdasarkan hasil *replay attack*, nilai *Attack Success Rate* (ASR) menurun dari 100% pada lingkungan *baseline* (VM1) menjadi 69,2% pada VM2 dan kembali menurun hingga 23,1% pada VM3. Penurunan yang terjadi pada VM2 terutama diperoleh melalui penerapan mekanisme pemantauan serta *containment* otomatis yang terbatas, khususnya perlindungan berbasis inotify yang berhasil mencegah *deployment web shell*. Pada VM3, penerapan kontrol yang berorientasi pada *Enforcement*, seperti *service hardening*, autentikasi SSH berbasis *public key*, penghapusan *Linux capability*, dan pembatasan akses yang lebih ketat, semakin menghambat rantai serangan dan mencegah penyerang melanjutkan aktivitasnya melewati tahap-tahap awal serangan.

Perbandingan antara VM2 dan VM3 juga menunjukkan adanya *trade-off* antara keamanan dan ketersediaan layanan. VM2 mengadopsi pendekatan *Detect-First* yang mempertahankan ketersediaan layanan inti sekaligus menyediakan visibilitas yang komprehensif terhadap aktivitas penyerang melalui mekanisme *logging*, *monitoring*, dan deteksi otomatis. Sebaliknya, VM3 lebih menitikberatkan pada pencegahan serangan melalui pembatasan akses yang lebih ketat dan kebijakan *Enforcement* yang lebih agresif, sehingga menghasilkan nilai ASR yang jauh lebih rendah. Pendekatan ini lebih sesuai diterapkan pada lingkungan yang memprioritaskan keamanan dibandingkan fleksibilitas layanan.

Meskipun hasil evaluasi menunjukkan bahwa *Overall Stage* pada sebagian besar pilar di VM2 dan VM3 masih berada pada tahap Traditional berdasarkan metode agregasi *majority*, *replay attack* memperlihatkan perbedaan ketahanan yang signifikan terhadap serangan. VM3 menghasilkan *Attack Success Rate* (ASR) sebesar 23,1%, jauh lebih rendah dibandingkan VM2 yang sebesar 69,2%. Temuan ini menunjukkan bahwa efektivitas mitigasi serangan tidak selalu tercermin secara langsung oleh kenaikan *tier* ZTMM, melainkan juga dipengaruhi oleh kedalaman implementasi kontrol pada fungsi-fungsi individual.

Hasil penelitian ini mengindikasikan bahwa pemilihan kontrol keamanan berbasis prinsip *Zero Trust* tidak hanya perlu mempertimbangkan tingkat kematangan yang ingin dicapai, tetapi juga harus memperhatikan kebutuhan operasional dari lingkungan yang dilindungi. Organisasi perlu menyeimbangkan aspek visibilitas, kemudahan penggunaan, ketersediaan layanan, dan tujuan keamanan sesuai dengan karakteristik lingkungan yang menjadi target implementasi. Temuan ini juga menunjukkan bahwa ZTMM lebih tepat digunakan sebagai kerangka evaluasi kematangan kontrol daripada sebagai indikator tunggal efektivitas pertahanan terhadap serangan. Oleh karena itu, sistem yang berada pada tingkat kematangan yang sama masih dapat menunjukkan tingkat ketahanan terhadap serangan yang berbeda, bergantung pada sejauh mana kontrol keamanan diterapkan dan ditegakkan. Dengan demikian, kombinasi pengukuran *Attack Success Rate* (ASR) dan evaluasi ZTMM memberikan sudut pandang yang saling melengkapi, yaitu efektivitas kontrol terhadap serangan serta tingkat kematangan implementasi kontrol itu sendiri.

Selain itu, hasil evaluasi menunjukkan bahwa mekanisme keamanan bawaan Linux dapat dimanfaatkan secara efektif untuk meningkatkan postur keamanan tanpa memerlukan solusi keamanan komersial yang kompleks. Komponen seperti nftables, fail2ban, auditd, inotify, *Linux capabilities*, serta kontrol akses berbasis SSH terbukti mampu memberikan kontribusi yang signifikan dalam membatasi pergerakan penyerang dan mengurangi peluang keberhasilan serangan. Temuan ini menunjukkan bahwa implementasi *Zero Trust* pada lingkungan Linux dapat dilakukan secara bertahap dengan memanfaatkan fitur-fitur yang telah tersedia secara *native* pada sistem operasi.

Penelitian ini menggunakan *CISA Zero Trust Maturity Model (ZTMM)* sebagai kerangka evaluasi karena tujuan penelitian bukan merancang arsitektur *Zero Trust* secara menyeluruh sebagaimana dijelaskan pada NIST SP 800-207, melainkan mengevaluasi tingkat kematangan implementasi kontrol keamanan berbasis prinsip *Zero Trust*. CISA

ZTMM menyediakan fungsi-fungsi evaluasi yang lebih operasional melalui lima pilar dan kapabilitas Cross-Cutting sehingga lebih sesuai digunakan untuk memetakan kontrol keamanan yang diterapkan pada lingkungan laboratorium penelitian ini.

Meskipun demikian, penelitian ini masih memiliki beberapa keterbatasan. Evaluasi dilakukan pada lingkungan laboratorium yang terkontrol dengan satu skenario *replay attack* yang direkonstruksi berdasarkan tahapan serangan yang telah diidentifikasi sebelumnya. Selain itu, lingkungan pengujian hanya terdiri atas satu mesin CTF (Amethysts) sehingga karakteristik kerentanan, konfigurasi layanan, dan *attack chain* yang dianalisis belum tentu merepresentasikan kondisi pada lingkungan *enterprise* maupun infrastruktur produksi yang lebih kompleks. Oleh karena itu, hasil yang diperoleh belum sepenuhnya merepresentasikan kompleksitas ancaman yang terdapat pada lingkungan produksi dengan variasi teknik serangan yang lebih luas.

Lebih lanjut, evaluasi tingkat kematangan dilakukan melalui interpretasi literal terhadap fungsi-fungsi pada CISA *Zero Trust Maturity Model* (ZTMM) v2.0 berdasarkan bukti implementasi yang tersedia pada lingkungan penelitian. Dengan demikian, hasil pemetaan mencerminkan tingkat kematangan kontrol yang berhasil diterapkan dalam ruang lingkup penelitian ini, dan belum dapat digeneralisasikan sebagai representasi implementasi *Zero Trust* pada lingkungan *enterprise* yang lebih kompleks.

Meskipun demikian, hasil penelitian menunjukkan bahwa penerapan kontrol keamanan berbasis prinsip *Zero Trust* menggunakan mekanisme keamanan bawaan Linux mampu meningkatkan ketahanan sistem terhadap *replay attack* yang direkonstruksi, sehingga pendekatan ini berpotensi menjadi acuan awal dalam penguatan keamanan pada lingkungan laboratorium maupun sistem dengan karakteristik serupa.

Di samping itu, beberapa kapabilitas yang direkomendasikan dalam CISA ZTMM, seperti *traffic encryption*, *Endpoint detection and response* (EDR), *secure software development lifecycle*, serta mekanisme perlindungan data yang lebih komprehensif, belum diimplementasikan karena berada di luar ruang lingkup penelitian.

5. Kesimpulan

Penelitian ini berhasil merekonstruksi *attack chain* sebanyak 13 tahapan pada mesin Amethysts yang digunakan dalam kompetisi *Attack-Defense* CTF KMIPN 2024 melalui pendekatan *post-mortem analysis*. Hasil analisis menunjukkan bahwa keberhasilan serangan dipengaruhi oleh kombinasi beberapa kelemahan, antara lain konfigurasi layanan yang tidak aman, mekanisme autentikasi yang lemah, kerentanan aplikasi web, serta *Linux capability* yang dikonfigurasi secara tidak tepat. Seluruh tahapan serangan berhasil dipetakan ke MITRE ATT&CK dan kerentanan yang dimanfaatkan dinilai menggunakan CVSS v3.1 sehingga dapat digunakan sebagai dasar penyusunan prioritas mitigasi.

Berdasarkan hasil analisis tersebut, penelitian ini merancang dan menerapkan kontrol keamanan berbasis prinsip *Zero Trust* menggunakan mekanisme keamanan bawaan Linux pada dua konfigurasi, yaitu *Detect-First* dan *Full Enforcement*. Hasil *replay attack chain* menunjukkan bahwa kontrol yang diterapkan mampu menurunkan *Attack Success Rate* (ASR) dari 100% pada lingkungan *baseline* menjadi 69,2% pada konfigurasi *Detect-First* dan 23,1% pada konfigurasi *Full Enforcement*. Hasil tersebut menunjukkan bahwa penerapan kontrol berdasarkan prinsip *Zero Trust* mampu meningkatkan ketahanan sistem dengan membatasi progresi *attack chain* yang diuji.

Evaluasi menggunakan CISA *Zero Trust Maturity Model* (ZTMM) v2.0 menunjukkan adanya peningkatan sejumlah fungsi menuju *tier* Initial, meskipun mayoritas fungsi masih berada pada *tier* Traditional. Temuan ini menunjukkan bahwa ASR dan ZTMM mengevaluasi aspek yang berbeda namun saling melengkapi, yaitu efektivitas kontrol dalam menghentikan serangan dan tingkat kematangan implementasi kontrol keamanan. Dengan demikian, peningkatan ketahanan terhadap serangan tidak selalu diikuti oleh peningkatan tingkat kematangan ZTMM karena kedua metrik memiliki tujuan evaluasi yang berbeda.

Penelitian ini merupakan studi kasus laboratorium pada satu mesin CTF (Amethysts), sehingga hasil yang diperoleh tidak dimaksudkan untuk digeneralisasikan secara langsung pada lingkungan *enterprise*. Selain itu, pengujian dilakukan menggunakan *replay* dari *attack chain* yang sama sehingga belum mengevaluasi variasi teknik serangan lain di luar skenario yang direkonstruksi.

Berdasarkan keterbatasan tersebut, penelitian selanjutnya disarankan untuk menguji kontrol berbasis prinsip *Zero Trust* pada lingkungan yang lebih kompleks, melibatkan beberapa *host* atau infrastruktur *enterprise*, menguji berbagai variasi *attack chain* maupun teknik serangan lain, serta mengevaluasi peningkatan kematangan hingga mencapai *tier* Advanced atau Optimal pada CISA ZTMM melalui

penerapan kapabilitas yang lebih komprehensif.

Ucapan Terima Kasih

Penulis menyampaikan penghargaan dan terima kasih yang sebesar-besarnya kepada para dosen pembimbing, seluruh dosen, serta Jurusan Teknik Informatika Politeknik Negeri Batam atas bimbingan, dukungan, dan arahan yang diberikan selama proses pelaksanaan dan penyelesaian penelitian ini.

Referensi

[1] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia," Id-SIRTII/CC, vol. 70, pp. 1–107, 2024.

[2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "*Zero Trust Architecture*," NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[3] Cybersecurity and Infrastructure Security Agency (CISA), "*Zero Trust Maturity Model* Version 2.0," CISA, USA, Apr. 2023. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[4] J. T. Tirstan, J. G. A., and Nelmiawati, "Analysis of Cyber Security Knowledge and Skills for Capture the Flag Competition," Jurnal Integrasi, vol. 14, no. 1, pp. 14–22, 2022. https://doi.org/10.30871/ji.v14i1.3986

[5] R. Fakhreja, K. Umam, K. Zahra, and I. S. Nurjiah, "National Cyber Defense: Analysis of Incident Severity Factors Using a Decision Tree," Jurnal Pertahanan, vol. 11, no. 1, pp. 1–15, 2025. https://doi.org/10.33172/jp.v11i1.19798

[6] W. Yeoh, M. Liu, M. Shore, and F. Jiang, "*Zero Trust* Cybersecurity: Critical Success Factors and a Maturity Assessment *Framework*," Computers & Security, vol. 133, 2023. https://doi.org/10.1016/j.cose.2023.103412

[7] Y. Kusnanto, M. A. Nugroho, and R. Kartadie, "Implementasi *Zero Trust Architecture* untuk Meningkatkan Keamanan Jaringan," Jurnal Informatika Polinema (JIPI), vol. 9, no. 4, pp. 2357–2364, 2024. https://doi.org/10.29100/jipi.v9i4.6943

[8] A. Rahman, E. Indrajit, A. Unggul, and E. Dazki, "Implementation of *Zero Trust* Security in MSME *Enterprise* Architecture," Sinkron, vol. 8, no. 3, pp. 2077–2087, 2024. https://doi.org/10.33395/sinkron.v8i3.13949

[9] Y. Ahmed, A. T. Asyhari, and M. A. Rahman, "A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats," Computers, Materials and Continua, vol. 67, no. 2, pp. 2497–2513, 2021. https://doi.org/10.32604/cmc.2021.014223

[10] MITRE Corporation, "MITRE ATT&CK *Enterprise* Matrix," 2024. [Online]. Available: https://attack.mitre.org/. [Accessed: Jun. 2026].

[11] D. Wackerly, W. Mendenhall, and R. L. Scheaffer, Mathematical Statistics with Applications, 7th ed. Belmont, CA, USA: Thomson Brooks/Cole, 2008.