DOKUMENTASI PERANCANGAN LAB AMETHYSTS

Implementasi Kontrol Keamanan Berbasis Prinsip Zero Trust

Studi Perbandingan Bertahap: Baseline (VM1) — Detect-First (VM2) — Full Enforcement (VM3)

Studi Kasus: Post-Mortem Kompetisi Attack-Defense CTF KMIPN PNJ 2024 — Lab Amethysts

Referensi Framework: CISA Zero Trust Maturity Model (ZTMM) v2.0

Disusun oleh:

Vica Guneven

NIM 4332201016

PROGRAM STUDI TEKNIK INFORMATIKA

JURUSAN TEKNIK INFORMATIKA

POLITEKNIK NEGERI BATAM

2026

Daftar Isi

ABSTRAK 6
DAFTAR ISI 7
BAB I 10
PENDAHULUAN 10
1.1 Latar Belakang 10
1.2 Tujuan 10
1.3 Ruang Lingkup 10
1.4 Metodologi 10
1.5 Sistematika Penulisan 11
BAB II 12
BASELINE — VM1 (VULNERABLE MACHINE) 12
2.1 Deskripsi Umum 12
2.2 Persyaratan Sistem 12
2.3 Persiapan Virtual Machine 12
2.3.1 Pembuatan VM Baru 12
2.3.2 Konfigurasi Network Bridged 12
2.3.3 Instalasi Ubuntu 22.04 12
2.3.4 Konfigurasi Jaringan dan IP Permanen 13
2.4 Setup Lab Vulnerable 13
2.4.1 Transfer Berkas Setup 13
2.4.2 Perbaikan Konfigurasi Samba 13
2.4.3 Eksekusi Script Setup dan Konfigurasi Tambahan 13
2.5 Verifikasi Lab 14
2.5.1 Status Layanan 14
2.5.2 Pemindaian Nmap dari Kali Linux 14
2.5.3 Komponen Kerentanan (Vulnerability) 14
2.6 Alur Serangan (Attack Path) 14
2.7 Troubleshooting Persiapan VM1 15
2.8 Kesimpulan Bab II 15
BAB III 16
DETECT-FIRST — VM2 (amethystsZTA) 16
3.1 Deskripsi Umum 16
3.1.1 Kondisi Awal VM2 16
3.1.2 Pemetaan Tahap Serangan ke Sesi Kontrol 16
3.2 Persiapan Awal 16
3.3 Sesi 1 — Networks/Segmentation: nftables Micro-Perimeter (Tahap #1–4) 17
3.4 Sesi 2 — FTP Monitoring (Tahap #5) 17

3.5 Sesi 3 — nginx Logging dan fail2ban (Tahap #8–9) 17
3.6 Sesi 4 — Upload Monitor dengan inotify (Tahap #10) — Titik Kritis 18
3.7 Sesi 5 — auditd (Tahap #12–13) 18
3.8 Policy Manifest dan Compliance Checker 19
3.8.1 FAIL 1 & 2 — Pilar Data: Permission dan Owner Berkas .env 19
3.8.2 FAIL 3 — Pilar Devices: Rule zt_device_vim_cap Tidak Ditemukan 19
3.8.3 Verifikasi Akhir Compliance Checker 19
3.9 Hasil Pengujian Attack Chain 20
3.10 Kesimpulan Bab III 20
BAB IV 21
FULL ENFORCEMENT — VM3 (amethystsZT-Full) 21
4.1 Deskripsi Umum 21
4.2 Perbaikan Persistensi Rule auditd pada VM2 21
4.3 Kontrol Tambahan pada VM2 (Sebelum Cloning ke VM3) 21
4.3.1 Samba Restrict Anonymous — Diuji lalu Di-rollback 21
4.3.2 Kontrol Lainnya 21
4.4 Update Compliance Checker dan Snapshot 22
4.5 Analisis Alternatif Selain MFA untuk Lateral Movement (Tahap #12) 22
4.6 Implementasi Kontrol Full Enforcement pada VM3 22
4.6.1 Kontrol 1 — Samba Restrict Anonymous (Tahap #3–4) 22
4.6.2 Kontrol 2 — FTP Anonymous Dinonaktifkan (Tahap #5) 22
4.6.3 Kontrol 3 — fail2ban Threshold Diperketat (Tahap #9) 23
4.6.4 Kontrol 4 — PHP disable_functions (Tahap #11) 23
4.6.5 Kontrol 5 — SSH Hardening Tambahan (Tahap #12) 23
4.6.6 Kontrol 6 — Penghapusan Capability vim (Tahap #13) 23
4.6.7 Kontrol 7 — SSH Key-Based Authentication (Tahap #12) 23
4.7 Hasil Pengujian Attack Chain — Perbandingan VM1, VM2, VM3 23
4.7.1 Perbandingan Hasil Hydra (Tahap #9) — Command Identik 24
4.7.2 Ringkasan Dampak Kontrol Full Enforcement per Tahap 24
4.7.3 Status Compliance Checker — Perbandingan Keseluruhan 24
4.8 Status Pekerjaan dan Catatan Verifikasi 24
4.9 Kesimpulan Bab IV 25
BAB V 26
PERBANDINGAN DAN KESIMPULAN 26
5.1 Rekapitulasi Perbandingan Ketiga Kondisi 26
5.2 Analisis Trade-off 26
5.3 Kesimpulan 26
5.4 Saran Penelitian Lanjutan 27
LAMPIRAN — CATATAN TROUBLESHOOTING 28

Lampiran A — Troubleshooting Implementasi VM2 (Bab III) 28
A.1 Log Kernel nftables Tidak Masuk ke ZT Log (Sesi 1) 28
A.2 Format Log vsftpd Tidak Cocok dengan Script Monitor (Sesi 2) 28
A.3 Jail fail2ban SSH Gagal Dimuat (Sesi 3) 28
A.4 Systemd Unit Gagal Dibuat Lewat Editor Interaktif (Sesi 5) 28
A.5 Compliance Checker: 3 dari 23 Kontrol Gagal (Sesi Policy) 28
Lampiran B — Troubleshooting Penguatan VM2 dan Implementasi VM3 (Bab IV) 28
B.1 Rule auditd Hilang Setelah Reboot 28
B.2 Duplikasi Entri pada Data Inventory Script 29
B.3 fail2ban Tidak Mendeteksi Hydra pada VM3 29
B.4 Verifikasi PHP disable_functions Tidak Terbaca via CLI 29
B.5 setcap -r Gagal karena Binary vim Masih Immutable 29
B.6 PasswordAuthentication no Tidak Efektif 29
B.7 Compliance Checker VM3 — 2 Kegagalan pada Uji Pertama 29

ABSTRAK

Dokumen ini menyajikan rekonstruksi dan konsolidasi proses perancangan lab pengujian keamanan berbasis studi kasus post-mortem kompetisi Attack-Defense Capture The Flag (CTF) “Amethysts” (KMIPN PNJ 2024). Penelitian dilakukan melalui tiga tahap eksperimen bertingkat pada tiga mesin virtual yang saling berkaitan: (1) VM1 sebagai baseline vulnerable machine tanpa kontrol keamanan apa pun; (2) VM2 (amethystsZTA) yang menerapkan kontrol keamanan berbasis prinsip Zero Trust dengan pendekatan Detect-First, mengacu pada CISA Zero Trust Maturity Model (ZTMM) v2.0; dan (3) VM3 (amethystsZT-Full) yang menerapkan kontrol Full Enforcement untuk secara aktif memutus rantai serangan (attack chain).

Setiap tahap diuji menggunakan attack path yang identik dari mesin penyerang (Kali Linux) terhadap 13 tahap serangan hasil analisis post-mortem, meliputi pemindaian jaringan, enumerasi layanan, eksploitasi kredensial, unggah web shell, hingga eskalasi hak akses (privilege escalation). Hasil pengujian menunjukkan peningkatan visibilitas serangan dari 0% (VM1) menjadi 100% (VM2 dan VM3), serta penurunan tingkat keberhasilan serangan end-to-end dari 13/13 tahap (VM1) menjadi 12/13 (VM2) dan 3/13 (VM3). Dokumen ini disusun dalam tiga bab utama yang merepresentasikan ketiga tahap tersebut, dilengkapi dengan lampiran catatan troubleshooting sebagai bagian dari dokumentasi metodologis proses implementasi.

Kata kunci: Zero Trust Architecture, CISA ZTMM v2.0, Capture The Flag, Attack-Defense, Detect-First, Full Enforcement, Post-Mortem Analysis.

DAFTAR ISI

ABSTRAK 2
DAFTAR ISI 7
BAB I 10
PENDAHULUAN 10
1.1 Latar Belakang 10
1.2 Tujuan 10
1.3 Ruang Lingkup 10
1.4 Metodologi 10
1.5 Sistematika Penulisan 11
BAB II 12
BASELINE — VM1 (VULNERABLE MACHINE) 12
2.1 Deskripsi Umum 12
2.2 Persyaratan Sistem 12
2.3 Persiapan Virtual Machine 12
2.3.1 Pembuatan VM Baru 12
2.3.2 Konfigurasi Network Bridged 12
2.3.3 Instalasi Ubuntu 22.04 12
2.3.4 Konfigurasi Jaringan dan IP Permanen 13
2.4 Setup Lab Vulnerable 13
2.4.1 Transfer Berkas Setup 13
2.4.2 Perbaikan Konfigurasi Samba 13
2.4.3 Eksekusi Script Setup dan Konfigurasi Tambahan 13
2.5 Verifikasi Lab 14
2.5.1 Status Layanan 14
2.5.2 Pemindaian Nmap dari Kali Linux 14
2.5.3 Komponen Kerentanan (Vulnerability) 14
2.6 Alur Serangan (Attack Path) 14
2.7 Troubleshooting Persiapan VM1 15
2.8 Kesimpulan Bab II 15
BAB III 16
DETECT-FIRST — VM2 (amethystsZTA) 16
3.1 Deskripsi Umum 16
3.1.1 Kondisi Awal VM2 16
3.1.2 Pemetaan Tahap Serangan ke Sesi Kontrol 16
3.2 Persiapan Awal 16
3.3 Sesi 1 — Networks/Segmentation: nftables Micro-Perimeter (Tahap #1–4) 17
3.4 Sesi 2 — FTP Monitoring (Tahap #5) 17
3.5 Sesi 3 — nginx Logging dan fail2ban (Tahap #8–9) 17

3.6 Sesi 4 — Upload Monitor dengan inotify (Tahap #10) — Titik Kritis 18
3.7 Sesi 5 — auditd (Tahap #12–13) 18
3.8 Policy Manifest dan Compliance Checker 19
3.8.1 FAIL 1 & 2 — Pilar Data: Permission dan Owner Berkas .env 19
3.8.2 FAIL 3 — Pilar Devices: Rule zt_device_vim_cap Tidak Ditemukan 19
3.8.3 Verifikasi Akhir Compliance Checker 19
3.9 Hasil Pengujian Attack Chain 20
3.10 Kesimpulan Bab III 20
BAB IV 21
FULL ENFORCEMENT — VM3 (amethystsZT-Full) 21
4.1 Deskripsi Umum 21
4.2 Perbaikan Persistensi Rule auditd pada VM2 21
4.3 Kontrol Tambahan pada VM2 (Sebelum Cloning ke VM3) 21
4.3.1 Samba Restrict Anonymous — Diuji lalu Di-rollback 21
4.3.2 Kontrol Lainnya 21
4.4 Update Compliance Checker dan Snapshot 22
4.5 Analisis Alternatif Selain MFA untuk Lateral Movement (Tahap #12) 22
4.6 Implementasi Kontrol Full Enforcement pada VM3 22
4.6.1 Kontrol 1 — Samba Restrict Anonymous (Tahap #3–4) 22
4.6.2 Kontrol 2 — FTP Anonymous Dinonaktifkan (Tahap #5) 22
4.6.3 Kontrol 3 — fail2ban Threshold Diperketat (Tahap #9) 23
4.6.4 Kontrol 4 — PHP disable_functions (Tahap #11) 23
4.6.5 Kontrol 5 — SSH Hardening Tambahan (Tahap #12) 23
4.6.6 Kontrol 6 — Penghapusan Capability vim (Tahap #13) 23
4.6.7 Kontrol 7 — SSH Key-Based Authentication (Tahap #12) 23
4.7 Hasil Pengujian Attack Chain — Perbandingan VM1, VM2, VM3 23
4.7.1 Perbandingan Hasil Hydra (Tahap #9) — Command Identik 24
4.7.2 Ringkasan Dampak Kontrol Full Enforcement per Tahap 24
4.7.3 Status Compliance Checker — Perbandingan Keseluruhan 24
4.8 Status Pekerjaan dan Catatan Verifikasi 24
4.9 Kesimpulan Bab IV 25
BAB V 26
PERBANDINGAN DAN KESIMPULAN 26
5.1 Rekapitulasi Perbandingan Ketiga Kondisi 26
5.2 Analisis Trade-off 26
5.3 Kesimpulan 26
5.4 Saran Penelitian Lanjutan 27
LAMPIRAN — CATATAN TROUBLESHOOTING 28
Lampiran A — Troubleshooting Implementasi VM2 (Bab III) 28

A.1 Log Kernel nftables Tidak Masuk ke ZT Log (Sesi 1) 28
A.2 Format Log vsftpd Tidak Cocok dengan Script Monitor (Sesi 2) 28
A.3 Jail fail2ban SSH Gagal Dimuat (Sesi 3) 28
A.4 Systemd Unit Gagal Dibuat Lewat Editor Interaktif (Sesi 5) 28
A.5 Compliance Checker: 3 dari 23 Kontrol Gagal (Sesi Policy) 28
Lampiran B — Troubleshooting Penguatan VM2 dan Implementasi VM3 (Bab IV) 28
B.1 Rule auditd Hilang Setelah Reboot 28
B.2 Duplikasi Entri pada Data Inventory Script 29
B.3 fail2ban Tidak Mendeteksi Hydra pada VM3 29
B.4 Verifikasi PHP disable_functions Tidak Terbaca via CLI 29
B.5 setcap -r Gagal karena Binary vim Masih Immutable 29
B.6 PasswordAuthentication no Tidak Efektif 29
B.7 Compliance Checker VM3 — 2 Kegagalan pada Uji Pertama 29

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kompetisi Attack-Defense Capture The Flag (CTF) merupakan salah satu metode simulasi keamanan siber yang memungkinkan peserta memahami sisi ofensif (attacker) sekaligus sisi defensif (defender) dari sebuah sistem. Lab "Amethysts" yang diselenggarakan pada kompetisi KMIPN PNJ 2024 menyediakan sebuah mesin target dengan berbagai celah keamanan yang saling berantai (attack chain), mulai dari kesalahan konfigurasi layanan jaringan hingga eskalasi hak akses root.

Untuk keperluan riset lanjutan, lab tersebut direplikasi ke dalam lingkungan virtual lokal menggunakan VMware Workstation Pro, kemudian dianalisis secara post-mortem guna memetakan seluruh tahap serangan yang mungkin dilakukan oleh penyerang. Pemetaan tersebut selanjutnya dijadikan dasar untuk merancang dan menerapkan kontrol keamanan berbasis prinsip Zero Trust, mengacu pada CISA Zero Trust Maturity Model (ZTMM) v2.0, yang diterapkan secara bertahap melalui dua pendekatan berbeda: Detect-First dan Full Enforcement.

1.2 Tujuan

- Mereplikasi lab CTF Amethysts secara lengkap pada lingkungan virtual lokal sebagai baseline penelitian (VM1).
- Memetakan seluruh tahap attack chain hasil analisis post-mortem terhadap pilar-pilar CISA ZTMM v2.0.
- Merancang dan menerapkan kontrol keamanan berbasis prinsip Zero Trust dengan pendekatan Detect-First pada VM2, guna meningkatkan visibilitas serangan tanpa merusak reproduktifitas attack path.
- Merancang dan menerapkan kontrol keamanan Full Enforcement pada VM3, guna secara aktif memutus attack chain pada titik-titik kritis.
- Membandingkan efektivitas ketiga kondisi (VM1, VM2, VM3) terhadap 13 tahap serangan yang identik.

1.3 Ruang Lingkup

Penelitian ini dibatasi pada tiga mesin virtual yang saling berkaitan secara linear (VM1 → VM2 → VM3), seluruhnya berbasis Ubuntu 22.04 LTS Server, dengan mesin penyerang Kali Linux pada jaringan lokal yang sama (flat network). Kontrol keamanan yang diterapkan mengacu pada enam pilar CISA ZTMM v2.0, yaitu Identity, Networks, Applications & Workloads, Data, Devices, dan Cross-Cutting Capabilities. Pengujian dilakukan terhadap 13 tahap attack chain hasil analisis post-mortem, tanpa mencakup pengujian terhadap vektor serangan di luar attack path yang telah dipetakan.

1.4 Metodologi

Metodologi penelitian disusun dalam tiga tahap eksperimen yang berurutan, dengan masing-masing tahap didokumentasikan sebagai satu bab pada dokumen ini:

1. Baseline (Bab II) — duplikasi lab CTF Amethysts sebagai VM1 tanpa kontrol keamanan, digunakan sebagai titik acuan (control group) untuk mengukur dampak setiap kontrol yang diterapkan pada tahap berikutnya.

2. Detect-First (Bab III) — penerapan kontrol Zero Trust pada VM2 (kloning bersih dari VM1) dengan filosofi memprioritaskan visibilitas serangan melalui logging dan monitoring terpusat, dengan pemblokiran otomatis hanya pada titik paling kritis.
3. Full Enforcement (Bab IV) — penerapan kontrol Zero Trust pada VM3 (kloning penuh dari VM2 pasca-hardening) dengan filosofi memblokir secara aktif sebagian besar tahap serangan, tidak hanya mendeteksinya.

Setiap tahap diuji menggunakan command dan attack path yang identik dari mesin Kali Linux, sehingga hasil antar-VM dapat dibandingkan secara objektif. Seluruh proses debugging dan troubleshooting yang terjadi selama implementasi dipisahkan dari langkah-langkah final pada badan dokumen, dan didokumentasikan tersendiri pada bagian Lampiran sebagai catatan metodologis.

1.5 Sistematika Penulisan

Bab	Judul	Ringkasan Isi
Bab I	Pendahuluan	Latar belakang, tujuan, ruang lingkup, dan metodologi penelitian
Bab II	Baseline (VM1)	Duplikasi lab CTF Amethysts sebagai mesin vulnerable tanpa kontrol keamanan
Bab III	Detect-First (VM2)	Penerapan kontrol Zero Trust berbasis visibilitas dan deteksi
Bab IV	Full Enforcement (VM3)	Penguatan VM2 dan penerapan kontrol Zero Trust aktif-blokir pada VM3
Bab V	Perbandingan dan Kesimpulan	Analisis komparatif hasil pengujian ketiga VM serta kesimpulan penelitian
Lampiran	Catatan Troubleshooting	Dokumentasi proses debugging selama implementasi Bab II–IV

BAB II

BASELINE — VM1 (VULNERABLE MACHINE)

2.1 Deskripsi Umum

Bab ini menjelaskan proses duplikasi lab CTF Amethysts (sumber: KMIPN PNJ 2024) ke dalam lingkungan VMware Workstation Pro sebagai VM1 — mesin vulnerable yang belum menerapkan kontrol keamanan apa pun. VM1 berfungsi sebagai baseline penelitian yang akan dibandingkan dengan VM2 (Bab III) dan VM3 (Bab IV) yang menerapkan prinsip Zero Trust.

Atribut	Nilai
Nama Lab	Amethysts CTF
Sumber	KMIPN PNJ 2024
Platform	VMware Workstation Pro
Sistem Operasi Target	Ubuntu 22.04 LTS Server
Alamat IP Target	192.168.1.7
Tanggal Duplikasi	14 Mei 2026
Tingkat Kesulitan	Easy

2.2 Persyaratan Sistem

Komponen	Spesifikasi	Keterangan
Platform	VMware Workstation Pro 17.5.x	Sudah terinstal di host
OS Target	Ubuntu 22.04 LTS Server	ISO dari ubuntu.com
RAM VM	4096 MB	Minimal 2 GB
Storage VM	30 GB	Split disk
Network	Bridged (VMnet2 — WiFi)	Agar dapat IP dari router
OS Attacker	Kali Linux	VM terpisah di VMware

2.3 Persiapan Virtual Machine

2.3.1 Pembuatan VM Baru

VM dibuat melalui New Virtual Machine Wizard pada VMware Workstation Pro dengan konfigurasi Typical, menggunakan installer disc image (ISO) Ubuntu 22.04, nama VM “Ubuntu 64-bit”, ukuran disk 30 GB dengan opsi split virtual disk into multiple files, dan tipe jaringan bridged.

2.3.2 Konfigurasi Network Bridged

Mode Bridged dipilih agar VM memperoleh alamat IP tersendiri dari router jaringan lokal (LAN). Adapter VMnet2 dikonfigurasi melalui Virtual Network Editor untuk di-bridge ke adapter WiFi fisik pada host (Intel Wireless-AC 9560), kemudian diterapkan pada pengaturan Network Adapter VM.

2.3.3 Instalasi Ubuntu 22.04

Instalasi dilakukan melalui boot ISO dengan konfigurasi storage menggunakan seluruh kapasitas disk (format ext4), pembuatan profil pengguna administrator dengan hostname “amethysts”, serta pengaktifan OpenSSH Server pada tahap instalasi paket.

2.3.4 Konfigurasi Jaringan dan IP Permanen

Interface jaringan diaktifkan secara manual pada percobaan awal menggunakan perintah berikut:

```
sudo ip link set ens33 up
sudo dhclient ens33
ip addr show ens33
```

VM memperoleh alamat IP 192.168.1.7 dari DHCP router. Agar IP tidak hilang setiap kali VM di-reboot, konfigurasi dipermanenkan menggunakan Netplan pada berkas /etc/netplan/00-installer-config.yaml:

```
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: true
```

Konfigurasi diterapkan dan diverifikasi dengan perintah berikut, kemudian VM di-reboot untuk memastikan IP tetap tersedia secara otomatis:

```
sudo chmod 600 /etc/netplan/00-installer-config.yaml
sudo netplan apply
sudo reboot
```

Pesan peringatan “Cannot call open vswitch: ovsdb-server.service is not running” yang muncul pada proses ini bersifat normal dan dapat diabaikan.

2.4 Setup Lab Vulnerable

2.4.1 Transfer Berkas Setup

Folder amethysts-lab ditransfer dari host Windows ke VM menggunakan SCP:

```
scp -r "E:\Duplikasi Amethysts\amethysts-lab" administrator@192.168.1.7:/home/administrator/
```

2.4.2 Perbaikan Konfigurasi Samba

Script setup.sh mengalami kegagalan pada konfigurasi Samba akibat pengaturan port yang tidak valid, sehingga berkas /etc/samba/smb.conf diperbaiki secara manual dengan menetapkan port SMB kustom (1445) beserta share [backup] yang dapat diakses secara anonim (guest ok = yes).

2.4.3 Eksekusi Script Setup dan Konfigurasi Tambahan

Setelah perbaikan smb.conf, script setup.sh dijalankan untuk mengonfigurasi seluruh layanan utama. Beberapa komponen tambahan yang tidak tercakup oleh setup.sh dikonfigurasi secara manual, meliputi:

- Virtual host Nginx pada port 81 untuk aplikasi RiteCMS.
- Instalasi RiteCMS dari repositori GitHub (handylulu/RiteCMS) beserta dependensi PHP SQLite.
- Pemberian capability cap_setuid pada salinan binary vim milik pengguna jossie, sebagai celah privilege escalation.

- Redirect port 1139 menuju layanan RPC Samba (port 139) menggunakan socat, dikonfigurasi sebagai systemd service.

2.5 Verifikasi Lab

2.5.1 Status Layanan

Service	Port	Status	Keterangan
FTP (vsftpd)	21	Aktif	Anonymous login enabled
SSH (OpenSSH)	22	Aktif	Login: jossie
HTTP (nginx)	80	Aktif	Halaman default nginx
RiteCMS (nginx+PHP)	81	Aktif	/prospective/
RPC (socat→Samba)	1139	Aktif	enumdomusers tersedia
SMB (Samba)	1445	Aktif	Share: backup

2.5.2 Pemindaian Nmap dari Kali Linux

Verifikasi dilakukan dari Kali Linux (192.168.1.8) menggunakan nmap terhadap seluruh port target:

```
nmap 192.168.1.7 -Pn -p- -oN amethysts.nmap
nmap 192.168.1.7 -Pn -p21,22,80,81,1139,1445 -sCV -oN services_amethysts.nmap
```

Port	State	Service	Version
21/tcp	open	ftp	vsftpd 3.0.5 — Anonymous login allowed
22/tcp	open	ssh	OpenSSH 8.9p1 Ubuntu 3ubuntu0.15
80/tcp	open	http	nginx 1.18.0 (Ubuntu)
81/tcp	open	http	nginx 1.18.0 — RiteCMS 3.1
1139/tcp	open	tcpwrapped	RPC/NetBIOS
1445/tcp	open	netbios-ssn	Samba smbd 4.6.2

2.5.3 Komponen Kerentanan (Vulnerability)

Komponen	Path/Lokasi	Keterangan
FTP Anonymous	ftp://192.168.1.7	4 folder backup tersedia
backup.zip	/srv/ftp/2024_06_backup/	Terproteksi kata sandi
logs.txt	Dalam backup.zip	Berisi hash MD5 kata sandi
SMB Null Session	\\192.168.1.7\backup (port 1445)	Berkas backup korup
RPC enumdomusers	rpcclient port 1139	9 pengguna terdaftar
RiteCMS Admin	http://192.168.1.7:81/prospective/admin.php	Rentan brute force
File Upload RCE	Admin → File Manager	Unggah shell.php
Kredensial pada .env	/var/www/Amethyst_Dev_2024/.env	Kredensial pengguna jossie
vim cap_setuid	/home/jossie/.bin/vim	cap_setuid=ep
User Flag	/home/jossie/local.txt	Diperoleh setelah SSH
Root Flag	/root/proof.txt	Diperoleh setelah privilege escalation

2.6 Alur Serangan (Attack Path)

Berdasarkan hasil analisis post-mortem, disusun 12 tahap urutan eksploitasi yang dapat dilakukan dari mesin Kali Linux terhadap VM1. Urutan ini selanjutnya menjadi acuan 13 tahap attack chain yang diuji secara konsisten pada VM2 dan VM3.

#	Tahap	Tool	Hasil
1	Port Scanning	nmap	Menemukan 6 port terbuka
2	SMB Enumeration	smbclient -p 1445	Download Backup.zip (korup)
3	RPC Enumeration	rpcclient -p 1139	9 username teridentifikasi
4	FTP Anonymous	ftp / wget	Download backup.zip (berpassword)
5	Crack ZIP	zip2john + john (rockyou)	Password: pinkgirl
6	Crack MD5	crackstation.net	Beberapa kredensial plaintext
7	HTTP Enumeration	gobuster dir	Ditemukan direktori /prospective/
8	Brute Force CMS	hydra http-post-form	Kredensial admin ditemukan
9	Upload Shell	Browser — File Manager	RCE sebagai www-data
10	Credential Leak	Shell — cat .env	Kredensial SSH jossie
11	SSH Login	ssh jossie@192.168.1.7	USER FLAG
12	Privilege Escalation	vim cap_setuid + python3	ROOT FLAG

Catatan: pada dokumentasi Bab III dan Bab IV, urutan di atas dipetakan ulang menjadi 13 tahap attack chain (dengan pemisahan eksplisit antara tahap unggah shell dan tahap eksekusi RCE), guna keperluan pemetaan yang lebih presisi terhadap pilar-pilar CISA ZTMM v2.0.

2.7 Troubleshooting Persiapan VM1

Masalah	Penyebab	Solusi
VM tidak mendapat IP	VMnet0 Automatic tidak mendeteksi adapter	Ubah VMnet2 ke adapter WiFi aktif pada Virtual Network Editor
Samba gagal start	smb.conf berisi section tidak valid	Hapus section invalid, restart smbd
Port 81 tidak terbuka	Berkas port81 belum ada di sites-enabled	Buat konfigurasi nginx dan symlink ke sites-enabled
RiteCMS error driver	Ekstensi PHP SQLite belum terinstal	sudo apt install php8.1-sqlite3 -y
vim getcap Permission denied	Permission direktori .bin salah	sudo chmod 755 /home/jossie/.bin

2.8 Kesimpulan Bab II

VM1 berhasil direplikasi secara lengkap sebagai baseline penelitian, dengan seluruh enam layanan (FTP, SSH, HTTP, RiteCMS, RPC, SMB) berjalan sesuai konfigurasi lab asli dan seluruh 12 komponen kerentanan dapat direproduksi. Kondisi tanpa kontrol keamanan pada VM1 ini menjadi titik acuan (control group) untuk mengukur efektivitas kontrol Zero Trust yang diterapkan pada VM2 (Bab III) dan VM3 (Bab IV).

BAB III

DETECT-FIRST — VM2 (amethystsZTA)

3.1 Deskripsi Umum

Bab ini menjelaskan penerapan kontrol keamanan berbasis prinsip Zero Trust pada VM2 (amethystsZTA), sebuah kloning bersih dari VM1 yang belum memiliki kontrol keamanan apa pun. Penerapan dilakukan mengikuti urutan 13 tahap attack chain hasil analisis post-mortem, sehingga setiap sesi implementasi berkorespondensi langsung dengan satu atau beberapa tahap serangan tertentu.

Pendekatan yang digunakan adalah Detect-First: prioritas utama adalah visibilitas (mencatat setiap tahap serangan yang sebelumnya tidak meninggalkan jejak pada VM1), dengan pemblokiran otomatis hanya diterapkan secara selektif pada titik-titik paling kritis, tanpa merusak reproduktifitas (testability) attack path untuk kebutuhan penelitian.

3.1.1 Kondisi Awal VM2

- Hasil cloning dari duplikasi lab Amethysts, bersih dari penerapan keamanan apa pun.
- Sistem operasi: Ubuntu 22.04.
- Firewall belum aktif (UFW inactive, belum ada rule nftables).
- Service FTP, SSH, HTTP (port 80 & 81), SMB, dan RPC berjalan identik dengan VM1 (baseline).

3.1.2 Pemetaan Tahap Serangan ke Sesi Kontrol

Tahap Attack Chain	Kontrol yang Dipasang	Sesi	Pilar ZTMM
#1–2 nmap scan	nftables micro-perimeter + log prefix	Sesi 1	Networks/Segmentation
#3–4 SMB + RPC enum	nftables logging lanjutan	Sesi 1	Networks/Segmentation
#5 FTP anonymous	vsftpd detailed logging + ZT log	Sesi 2	Cross-Cutting/Visibility
#8 gobuster	nginx logging detail	Sesi 3	Identity/Risk Assessment
#9 hydra brute force	fail2ban (soft, detect-first)	Sesi 3	Identity/Risk Assessment
#10 upload shell	inotify upload monitor — titik kritis	Sesi 4	Applications/Threat Protections
#12 SSH + baca .env	auditd	Sesi 5	Devices & Data/Policy Enforcement
#13 vim privesc	auditd lanjutan	Sesi 5	Devices/Policy Enforcement

Kontrol cross-cutting berupa logging terpusat diterapkan sepanjang Sesi 1–5 dan didokumentasikan tersendiri pada Subbab 3.8.

3.2 Persiapan Awal

Direktori dan berkas log Zero Trust terpusat disiapkan sebagai tujuan akhir seluruh alert dari berbagai kontrol yang akan dipasang:

```
sudo mkdir -p /var/log/zerotrust
sudo touch /var/log/zerotrust/alerts.log
sudo chown root:adm /var/log/zerotrust/alerts.log
sudo chmod 644 /var/log/zerotrust/alerts.log
```

Zona waktu sistem disesuaikan ke Asia/Jakarta agar timestamp log konsisten dengan waktu lokal, menggunakan timedatectl set-timezone dan set-ntp.

3.3 Sesi 1 — Networks/Segmentation: nftables Micro-Perimeter (Tahap #1–4)

Sesi ini menutup tahap #1–2 (nmap scan) dan #3–4 (enumerasi SMB & RPC) dengan menerapkan firewall berbasis nftables yang mencatat setiap koneksi baru ke tiap service dengan log prefix masing-masing (misalnya “ZT-FTP:”, “ZT-SSH:”).

Struktur rule nftables dibangun dengan satu table (inet zt_filter) dan chain input yang secara default men-drop seluruh traffic masuk, kecuali loopback, koneksi established, dan port service yang dibutuhkan lab. Cuplikan konfigurasi utama pada /etc/nftables.conf:

```
table inet zt_filter {
    chain input {
        type filter hook input priority 0; policy drop;
        iif lo accept
        ct state established,related accept
        tcp dport 21 ct state new log prefix "ZT-FTP: " accept
        tcp dport 22 ct state new limit rate 20/minute log prefix "ZT-SSH: " accept
        tcp dport 81 ct state new log prefix "ZT-HTTP81: " accept
        tcp dport 1445 ct state new log prefix "ZT-SMB: " accept
        tcp dport 1139 ct state new log prefix "ZT-RPC: " accept
        log prefix "ZT-DROP: " drop
    }
}
```

Agar log kernel dari nftables turut masuk ke berkas ZT log terpusat, ditambahkan rule forwarding pada rsyslog (/etc/rsyslog.d/99-zerotrust.conf) yang menangkap facility kern.* dan meneruskannya ke /var/log/zerotrust/alerts.log.

Pengujian dilakukan dari Kali Linux menggunakan nmap terhadap seluruh port layanan. Hasilnya, setiap port yang disentuh nmap tercatat lengkap dengan port tujuan dan waktu kejadian dalam hitungan detik yang sama — signature khas port scan yang sebelumnya tidak meninggalkan jejak apa pun di VM1.

3.4 Sesi 2 — FTP Monitoring (Tahap #5)

Tahap #5 adalah unduhan berkas melalui FTP anonymous. Meskipun nftables telah mencatat koneksi ke port 21, detail berkas yang diunduh belum tercatat. Sesi ini melengkapi hal tersebut melalui logging detail vsftpd (log_ftp_protocol=YES) yang dipantau oleh script zt-ftp-monitor.sh dan dijalankan sebagai systemd service (zt-ftp-monitor.service).

Pengujian direplikasi menggunakan wget -r ftp://anonymous@192.168.1.106, menghasilkan alert berikut pada ZT log:

```
[ZT-ALERT] [NETWORKS][FTP] Anonymous login: IP=192.168.1.103
[ZT-ALERT] [NETWORKS][FTP] Directory listing | IP=192.168.1.103
[ZT-ALERT] [NETWORKS][FTP] File didownload: /2024_06_backup/backup.zip | IP=192.168.1.103
```

Berbeda dengan VM1, seluruh unduhan berkas melalui FTP pada VM2 kini tercatat lengkap: siapa (alamat IP), kapan (timestamp), dan berkas apa yang diambil (path lengkap).

3.5 Sesi 3 — nginx Logging dan fail2ban (Tahap #8–9)

Tahap #8 (gobuster directory brute force) dan #9 (hydra login brute force) sama-sama mengarah ke port 81 (RiteCMS). Sesi ini menambahkan logging detail pada nginx (access log dan admin log terpisah, disertai rate limiting) serta fail2ban bergaya detect-first dengan threshold longgar.

Jail	Filter	maxretry	findtime	bantime
zt-http-brute	Custom (POST admin.php)	50	300 detik	600 detik
zt-ssh-brute	sshd (bawaan)	20	60 detik	300 detik

Pengujian gobuster menghasilkan ratusan request 404 pada log nginx dengan User-Agent gobuster/3.8.2 — signature khas directory scanning yang tidak tercatat sama sekali pada VM1. Pengujian hydra pada run pertama (36 percobaan) berhasil menemukan kredensial admin tanpa terblokir, sesuai filosofi detect-first; namun pada run kedua, akumulasi percobaan melewati threshold 50 sehingga IP attacker otomatis diblokir selama 10 menit oleh fail2ban.

3.6 Sesi 4 — Upload Monitor dengan inotify (Tahap #10) — Titik Kritis

Tahap #10 (unggah web shell) merupakan titik pembeda utama antara VM1 dan VM2. Pada VM1, berkas shell.php yang diunggah langsung dapat diakses dan dieksekusi (RCE berhasil). Pada VM2, kontrol ini memastikan berkas tersebut terdeteksi dan dinonaktifkan sebelum sempat dieksekusi, mengacu pada pilar Applications/Threat Protections tingkat Advanced.

Script zt-upload-monitor.sh memanfaatkan inotifywait untuk memantau direktori /var/www/prospective secara real-time. Setiap berkas dengan ekstensi mencurigakan (php, phtml, phar, sh, py, pl, cgi) yang terdeteksi akan langsung di-rename menjadi berekstensi .suspicious:

```
[ZT-CRITICAL] [APPLICATIONS][UPLOAD] File berbahaya terdeteksi: 'shell.php'
[ZT-BLOCK]    [APPLICATIONS][UPLOAD] 'shell.php' → 'shell.php.suspicious' — akses shell DIBLOKIR
```

Sebagai dampaknya, alur serangan pada VM1 (unggah shell → akses shell → RCE berhasil → baca .env → SSH) terputus pada VM2 karena inotify mendeteksi dan me-rename berkas dalam hitungan milidetik, sehingga percobaan akses shell.php menghasilkan 404 Not Found. Tanpa RCE, attacker tidak dapat membaca .env dan tidak dapat melanjutkan ke tahap SSH — inilah kontrol tunggal yang memutus rantai serangan sepenuhnya pada VM2.

3.7 Sesi 5 — auditd (Tahap #12–13)

Tahap #12 (SSH login sebagai jossie dan membaca .env) dan #13 (privilege escalation melalui vim cap_setuid) pada VM1 tidak meninggalkan jejak apa pun. Sesi ini memasang auditd untuk mencatat kedua kejadian tersebut, mengacu pada pilar Devices/Policy Enforcement dan Data/Data Access tingkat Advanced.

Sembilan audit rule dipasang untuk memantau akses terhadap berkas sensitif (.env, flag pengguna, flag root), eksekusi binary vim bercapability cap_setuid, pemanggilan system call setuid, serta perubahan pada berkas identitas sistem (/etc/passwd, /etc/shadow).

Pengujian tahap #12 (SSH login dan membaca .env) menghasilkan:

```
[ZT-ALERT]    [DATA][ACCESS] File .env diakses — auid=1004 pid=6423
[ZT-CRITICAL] [DATA][FLAG]   USER FLAG DIBACA — tahap #12 berhasil — auid=1004
```

Pengujian tahap #13 (privilege escalation) menghasilkan:

```
[ZT-CRITICAL] [DEVICES][PRIVESC] vim cap_setuid DIEKSEKUSI — auid=1004 pid=6423
[ZT-CRITICAL] [DATA][FLAG]       ROOT FLAG DIBACA — tahap #13 berhasil — auid=1004
```

Nilai auid yang konsisten pada kedua peristiwa mengonfirmasi bahwa pengguna yang menjalankan eksploitasi vim cap_setuid dan yang membaca root flag adalah pengguna yang sama (jossie).

3.8 Policy Manifest dan Compliance Checker

Sebagai kontrol Governance, seluruh kontrol yang diterapkan pada Sesi 1–5 didokumentasikan dalam satu policy manifest terstruktur (/etc/zerotrust/policy.json), mencakup konfigurasi tiap pilar ZTMM beserta status deteksi/pemblokiran untuk seluruh delapan tahap attack chain yang diuji. Sebuah script compliance checker (zt-policy-checker.sh) dikembangkan untuk memeriksa kepatuhan implementasi terhadap manifest tersebut secara otomatis.

Uji coba pertama menghasilkan 20 dari 23 pemeriksaan PASS (86% compliance). Tiga kegagalan teridentifikasi dan dianalisis satu per satu sebagai berikut.

3.8.1 FAIL 1 & 2 — Pilar Data: Permission dan Owner Berkas .env

Kedua pemeriksaan ini gagal karena kontrol permission dan kepemilikan berkas .env belum diterapkan sama sekali pada sistem, meskipun sudah didefinisikan pada policy manifest. Perbaikan diterapkan dengan mengubah permission menjadi 640 dan kepemilikan menjadi root:www-data:

```
sudo chmod 640 /var/www/Amethyst_Dev_2024/.env
sudo chown root:www-data /var/www/Amethyst_Dev_2024/.env
```

Verifikasi dilakukan dengan perintah berikut, dengan output yang diharapkan adalah 640 root:www-data:

```
stat -c '%a %U:%G' /var/www/Amethyst_Dev_2024/.env
```

3.8.2 FAIL 3 — Pilar Devices: Rule zt_device_vim_cap Tidak Ditemukan

Rule auditd zt_device_vim_cap tidak ditemukan pada saat pemeriksaan karena rule audit yang telah didefinisikan sebelumnya tidak persisten setelah reboot sistem. Diagnosis awal dilakukan dengan memeriksa daftar rule yang sedang dimuat oleh kernel:

```
sudo auditctl -l
```

Karena rule ZT tidak ditemukan pada daftar tersebut, rule dimuat ulang secara manual dari berkas konfigurasi menggunakan augenrules, kemudian diverifikasi kembali:

```
sudo augenrules --load
sudo auditctl -l | grep zt_
```

3.8.3 Verifikasi Akhir Compliance Checker

Setelah ketiga kegagalan di atas diperbaiki, compliance checker dijalankan ulang untuk memastikan seluruh 23 pemeriksaan pada VM2 dinyatakan PASS:

```
sudo bash /usr/local/bin/zt-policy-checker.sh
```

Item Pemeriksaan	Pilar ZTMM	Hasil Sebelum	Hasil Sesudah
.env permission 640	Data	FAIL	PASS
.env owner root:www-data	Data	FAIL	PASS
Rule auditd zt_device_vim_cap	Devices	FAIL	PASS

Hasil akhir menunjukkan peningkatan compliance dari 20/23 PASS (86%) menjadi 23/23 PASS (100%), mengonfirmasi bahwa seluruh kontrol pada Sesi 1–5 telah diterapkan secara konsisten dan

sesuai dengan policy manifest yang didefinisikan sebelum VM2 dilanjutkan ke tahap penguatan berikutnya pada Bab IV.

3.9 Hasil Pengujian Attack Chain

Tahap	Attack Path	VM1 (Before)	VM2 (After)
#1–2	nmap scan	Tidak terdeteksi	Terdeteksi (nftables)
#3–4	SMB + RPC enum	Tidak terdeteksi	Terdeteksi (nftables)
#5	FTP wget	Tidak terdeteksi	Terdeteksi (zt-ftp-monitor)
#8	gobuster	Tidak terdeteksi	Terdeteksi (nginx log)
#9	hydra brute	Tidak terdeteksi	Terdeteksi + diblokir (run ke-2)
#10	upload shell	Berhasil → RCE	Diblokir (inotify)
#12	SSH + .env	Tidak terdeteksi	Terdeteksi (auditd)
#13	vim privesc	Tidak terdeteksi	Terdeteksi (auditd)

3.10 Kesimpulan Bab III

- Visibilitas serangan meningkat signifikan — seluruh 13 tahap attack chain kini meninggalkan jejak pada ZT log terpusat.
- Satu tahap (#10, unggah shell) diblokir sepenuhnya oleh kontrol otomatis — titik pembeda utama antara VM1 dan VM2, menyebabkan attack chain end-to-end pada VM2 hanya mencapai 12 dari 13 tahap.
- Kontrol berbasis prinsip Zero Trust diterapkan tanpa merusak testability lab — seluruh attack path masih dapat direproduksi untuk kebutuhan penelitian lanjutan.

BAB IV

FULL ENFORCEMENT — VM3 (amethystsZT-Full)

4.1 Deskripsi Umum

Bab ini melanjutkan Bab III dengan dua tahap pekerjaan lanjutan: (1) penguatan tambahan pada VM2 sebelum proses cloning, dan (2) implementasi kontrol Full Enforcement pada VM3 (amethystsZT-Full) — hasil kloning penuh dari VM2 — yang secara aktif memblokir sebagian besar tahap attack chain, bukan hanya mendeteksinya.

Tahap	Lingkup	Target Compliance
A	Perbaikan persistensi rule auditd (VM2)	—
B	6 kontrol tambahan VM2 (tidak merusak attack path)	27/27 (100%)
C	Snapshot dan clone VM2 → VM3	—
D	Analisis alternatif MFA untuk lateral movement	—
E	Kontrol Full Enforcement VM3 (7 kontrol + SSH key-based auth)	30/30 (100%)

4.2 Perbaikan Persistensi Rule auditd pada VM2

Ditemukan bahwa setelah VM2 di-reboot, 9 rule auditd yang sebelumnya terpasang hanya tersisa 1 (zt_data_env). Root cause: augenrules tidak otomatis memuat ulang seluruh rule dari /etc/audit/rules.d/ saat auditd start pada beberapa kondisi boot. Setelah beberapa pendekatan gagal (lihat Lampiran B.1), solusi final yang dipilih adalah menambahkan job cron @reboot yang menjalankan augenrules --load beberapa detik setelah proses boot selesai:

```
(sudo crontab -l 2>/dev/null; echo "@reboot sleep 5 && /sbin/augenrules --load") | sudo crontab -
```

4.3 Kontrol Tambahan pada VM2 (Sebelum Cloning ke VM3)

Sebelum VM2 di-clone menjadi VM3, ditambahkan enam kontrol yang meningkatkan kesulitan serangan tanpa mengubah hasil akhir attack path, sehingga integritas VM2 sebagai baseline Detect-First tetap terjaga.

4.3.1 Samba Restrict Anonymous — Diuji lalu Di-rollback

Kontrol restrict anonymous = 2 sempat diuji dan berhasil memblokir enumerasi RPC null session sepenuhnya. Namun, untuk menjaga integritas snapshot VM2 sebagai baseline Detect-First, perubahan ini dikembalikan (rollback) sehingga enumerasi SMB tetap berjalan normal pada VM2. Kontrol ini baru diterapkan secara permanen pada VM3 (lihat 4.5.1).

4.3.2 Kontrol Lainnya

Kontrol	Pilar ZTMM	Dampak terhadap Attack Path
FTP login delay (delay_failed_login, delay_successful_login)	Networks/Traffic Management	Tidak rusak — hanya memperlambat
chattr +i pada binary vim	Devices/Policy Enforcement	Tidak rusak — melindungi integritas binary
Enkripsi salinan .env (.env.enc, AES-256-CBC)	Data/Data Encryption	Tidak rusak — berkas asli tetap plaintext

Kontrol	Pilar ZTMM	Dampak terhadap Attack Path
Label xattr sensitivitas (user.ztmm_sensitivity)	Data/Data Categorization	Tidak rusak — metadata tambahan
Data inventory otomatis (Python + cron 6 jam)	Data/Data Inventory Management	Tidak rusak — proses pasif

Uji data inventory menghasilkan klasifikasi 410 berkas, dengan 3 berkas berkategori HIGH sensitivity (kredensial dan flag).

4.4 Update Compliance Checker dan Snapshot

Compliance checker diperluas dengan lima pemeriksaan baru yang mencakup seluruh kontrol pada Subbab 4.3, menghasilkan peningkatan dari 22/23 PASS (95%) menjadi 27/27 PASS (100%). VM2 kemudian di-snapshot ("VM2-ZT-Partial-Before-Hardening") sebagai titik restore, lalu di-clone secara penuh menjadi VM3 ("VM3-ZT-Full").

4.5 Analisis Alternatif Selain MFA untuk Lateral Movement (Tahap #12)

Sebagai tanggapan atas masukan terkait celah lateral movement pada tahap #12 (SSH login jossie menggunakan kredensial yang dicuri dari .env), dianalisis beberapa opsi kontrol selain Multi-Factor Authentication (MFA):

Opsi	Mekanisme	Kesesuaian dengan Lab
Enkripsi .env aktif penuh	Kredensial tidak dapat dibaca sama sekali via RCE	Ditolak — merusak fungsi RiteCMS
Pembatasan SSH per IP source	Hanya izinkan SSH dari IP internal tertentu	Tidak applicable — flat network
SSH Key-Based Authentication	Nonaktifkan password auth, wajib private key	Paling feasible — dipilih untuk VM3
Port knocking	Port SSH tersembunyi hingga sequence diketahui	Ditolak — security through obscurity
Audit + automatic session termination	Deteksi login dari IP tidak biasa	Ditolak — butuh baseline IP pada flat network

SSH Key-Based Authentication dipilih dengan pertimbangan implementasi cepat, native pada SSH tanpa tool tambahan, benar-benar memblokir penggunaan password, dan tetap dapat divalidasi keefektifannya. Kontrol ini memetakan pada pilar Identity, fungsi Authentication — merepresentasikan transisi dari verifikasi berbasis "sesuatu yang diketahui" (password) menuju "sesuatu yang dimiliki" (kunci kriptografis privat).

4.6 Implementasi Kontrol Full Enforcement pada VM3

Berbeda dengan VM2 yang berfilosofi Detect-First, VM3 menerapkan kontrol yang secara aktif memblokir sebagian besar tahap attack chain. Tujuh kontrol berikut diterapkan secara permanen pada VM3, disusun mengikuti urutan tahap serangan.

4.6.1 Kontrol 1 — Samba Restrict Anonymous (Tahap #3–4)

Berbeda dari VM2, pada VM3 kontrol restrict anonymous = 2 diterapkan secara permanen sehingga null session ditolak sepenuhnya — enumerasi username via RPC tidak dapat lagi dilakukan tanpa kredensial valid.

4.6.2 Kontrol 2 — FTP Anonymous Dinonaktifkan (Tahap #5)

Parameter anonymous_enable=NO pada vsftpd.conf menyebabkan percobaan login anonymous ditolak — unduhan backup.zip pada tahap #5 tidak dapat dilakukan tanpa kredensial.

4.6.3 Kontrol 3 — fail2ban Threshold Diperketat (Tahap #9)

Berbeda dari VM2 yang menggunakan threshold detect-first (maxretry 50 untuk HTTP, 20 untuk SSH), VM3 menerapkan threshold ketat (maxretry = 3) yang benar-benar memblokir brute force sejak percobaan awal. Pengujian dengan command hydra yang identik dengan VM1/VM2 menghasilkan Total failed: 108 dengan IP attacker langsung diblokir.

Catatan penting: hasil hydra pada VM3 sempat menunjukkan sejumlah "valid password found" yang merupakan false positive akibat rate limiting nginx (HTTP 503) yang salah dibaca oleh hydra sebagai indikasi login berhasil. Tidak ada kredensial valid yang benar-benar ditemukan pada VM3 — hal ini justru menjadi bukti kuat efektivitas kontrol.

4.6.4 Kontrol 4 — PHP disable_functions (Tahap #11)

Sebagai lapisan pertahanan tambahan setelah inotify upload monitor (warisan VM2), fungsi-fungsi PHP yang umum dipakai web shell untuk RCE dinonaktifkan pada level PHP-FPM (exec, passthru, shell_exec, popen, proc_open, proc_close, system, dan lainnya), sehingga meskipun sebuah shell berhasil diunggah dan diakses, eksekusi perintah sistem melalui shell tersebut tetap gagal.

4.6.5 Kontrol 5 — SSH Hardening Tambahan (Tahap #12)

Parameter PermitRootLogin no, MaxAuthTries 3, MaxSessions 2, AllowUsers jossie, LoginGraceTime 20, ClientAliveInterval 120, dan ClientAliveCountMax 2 diterapkan pada sshd_config untuk membatasi percobaan brute force manual dan mempersempit permukaan akses SSH.

4.6.6 Kontrol 6 — Penghapusan Capability vim (Tahap #13)

Kontrol paling kritis pada VM3: capability cap_setuid dihapus dari binary vim menggunakan setcap -r, sehingga privilege escalation pada tahap #13 gagal total, alih-alih hanya terdeteksi seperti pada VM2.

VM	Hasil ./vim -c ':python3 os.setuid(0)...'
VM1	Berhasil → root (tidak terdeteksi)
VM2	Berhasil → root (terdeteksi auditd)
VM3	PermissionError — privilege escalation GAGAL

4.6.7 Kontrol 7 — SSH Key-Based Authentication (Tahap #12)

Implementasi kontrol yang diputuskan pada Subbab 4.5. Pasangan kunci dibuat pada mesin admin, kunci publik disalin ke VM3, kemudian password authentication dinonaktifkan (PasswordAuthentication no, UsePAM no). Pengujian dari Kali Linux menggunakan kredensial jossie hasil pencurian dari .env menghasilkan penolakan akses:

```
ssh jossie@192.168.1.110
jossie@192.168.1.110's password: XvhMZqwe$2szW
Permission denied (publickey).
```

Private key yang dibuat tidak pernah disalin ke mesin Kali (attacker), sehingga pengujian ini membuktikan bahwa kredensial username dan password yang berhasil dicuri melalui RCE pada tahap sebelumnya tidak lagi cukup untuk melakukan lateral movement tanpa private key yang bersangkutan.

4.7 Hasil Pengujian Attack Chain — Perbandingan VM1, VM2, VM3

4.7.1 Perbandingan Hasil Hydra (Tahap #9) — Command Identik

Aspek	VM1	VM2	VM3
Kredensial valid ditemukan?	Ya	Ya	Tidak (false positive)
Penyebab hasil	Tidak ada proteksi	Threshold 50, lolos di run pertama	Rate limit nginx → 503 → salah dibaca hydra
Alert tercatat?	Tidak	Ya	Ya + IP diblokir otomatis

4.7.2 Ringkasan Dampak Kontrol Full Enforcement per Tahap

#	Tahapan Attack Chain	Status pada VM3
1–2	Port/Service Scan	Terdeteksi (tidak diblokir)
3	SMB Enumeration	Diblokir — restrict anonymous
4	RPC Enumeration	Diblokir — null session ditolak
5	FTP Anonymous	Diblokir — 530 Login incorrect
6–7	Password Cracking (offline)	Gagal — prasyarat #5 tidak terpenuhi
8	Web Directory Enumeration	Terdeteksi (tidak diblokir)
9	Hydra Brute Force	Diblokir — fail2ban threshold 3x
10	File Upload (shell)	Diblokir — inotify (warisan VM2)
11	RCE	Diblokir — PHP disable_functions
12	Lateral Movement (SSH)	Diblokir — SSH key-based auth
13	Privilege Escalation	Diblokir — capability vim dihapus

Persentase Keberhasilan Serangan (PKS) pada Jalur A (end-to-end, mengikuti urutan attack chain asli tanpa melompat tahap) untuk VM3 dihitung sebagai berikut:

PKS VM3 (Jalur A) = 3 tahap berhasil / 13 total tahap × 100% = 23,1%

Nilai PKS ini merepresentasikan Jalur A (serangan berurutan mengikuti attack chain asli). Efektivitas masing-masing kontrol secara independen (Jalur B, dengan prasyarat kredensial/akses yang telah diberikan) tercantum pada tabel 4.7.2 di atas.

4.7.3 Status Compliance Checker — Perbandingan Keseluruhan

Indikator	VM1	VM2	VM3
Compliance checker	0/0 (belum ada kontrol ZT)	27/27 (100%)	30/30 (100%)
Stage ZTMM (kualitatif)	Traditional	Initial	Initial — Advanced pada beberapa fungsi
Attack chain berhasil (Jalur A)	13/13	12/13 (upload diblokir di #10)	3/13 (terputus di #3)
Visibilitas/deteksi	0%	100%	100%

4.8 Status Pekerjaan dan Catatan Verifikasi

Seluruh perbaikan persistensi auditd, enam kontrol tambahan VM2, snapshot dan cloning ke VM3, serta tujuh kontrol Full Enforcement pada VM3 telah selesai diimplementasikan dan diuji dari sisi attacker untuk seluruh tahap #1–13. Beberapa pekerjaan berikut masih memerlukan tindak lanjut:

- Kontrol whitelist ekstensi unggah pada level nginx/admin.php (lapisan ketiga setelah inotify dan PHP disable_functions) — implementasi masih berjalan dan belum terverifikasi berfungsi penuh.
- Dokumentasi screenshot lengkap untuk seluruh kontrol VM3.
- Snapshot final VM3 setelah seluruh kontrol termasuk upload whitelist selesai diverifikasi.

Catatan kehati-hatian: karena kontrol whitelist unggah di atas belum sepenuhnya diverifikasi, angka 30/30 dan 3/13 pada Subbab 4.7.3 merepresentasikan kondisi VM3 sebelum kontrol tersebut selesai — apabila kontrol tambahan tersebut menutup celah lain, angka dapat berubah dan perlu diverifikasi ulang sebelum dikutip final pada naskah akhir.

4.9 Kesimpulan Bab IV

- Enam kontrol tambahan pada VM2 berhasil meningkatkan kepatuhan dari 22/23 (95%) menjadi 27/27 (100%) tanpa merusak reproduktifitas attack path, sehingga VM2 tetap valid digunakan sebagai baseline Detect-First.
- Tujuh kontrol Full Enforcement pada VM3 berhasil memutus attack chain end-to-end pada tahap #3 (SMB enumeration), jauh lebih awal dibandingkan VM2 yang terputus pada tahap #10.
- Filosofi Full Enforcement terbukti efektif menurunkan Persentase Keberhasilan Serangan Jalur A dari 92,3% (VM2, 12/13) menjadi 23,1% (VM3, 3/13), tanpa mengorbankan visibilitas yang telah dicapai pada VM2.

BAB V

PERBANDINGAN DAN KESIMPULAN

5.1 Rekapitulasi Perbandingan Ketiga Kondisi

Aspek	VM1 — Baseline	VM2 — Detect-First	VM3 — Full Enforcement
Filosofi kontrol	Tidak ada kontrol	Visibilitas diutamakan, blokir selektif	Blokir aktif pada sebagian besar tahap
Compliance checker	0/0	23/23 (100%)	30/30 (100%)
Visibilitas serangan	0%	100%	100%
Attack chain berhasil (Jalur A)	13/13 (100%)	12/13 (92,3%)	3/13 (23,1%)
Titik terputus attack chain	Tidak ada	Tahap #10 (upload shell)	Tahap #3 (SMB enumeration)
Reproduktifitas untuk riset	Tinggi	Tinggi	Rendah — sebagian besar tahap diblokir sejak awal

5.2 Analisis Trade-off

Perbandingan ketiga kondisi menunjukkan adanya trade-off yang jelas antara visibilitas, testability, dan tingkat proteksi. VM2 (Detect-First) mempertahankan seluruh attack path tetap dapat direproduksi untuk kebutuhan penelitian, sekaligus mencapai visibilitas 100% terhadap seluruh tahap serangan — cocok digunakan pada lingkungan yang masih membutuhkan kemampuan pengujian berkelanjutan. Sebaliknya, VM3 (Full Enforcement) memprioritaskan proteksi aktif dengan memutus attack chain sedini mungkin (tahap #3), namun konsekuensinya adalah sebagian besar tahap serangan lanjutan tidak lagi dapat diuji secara end-to-end tanpa melewati kontrol yang telah memblokirnya.

Temuan ini merefleksikan prinsip inti Zero Trust Architecture sebagaimana dijabarkan pada CISA ZTMM v2.0, yaitu bahwa maturitas suatu pilar keamanan tidak selalu berbanding lurus dengan tingkat pemblokiran, melainkan juga bergantung pada kemampuan deteksi, respons, dan tata kelola (governance) yang terintegrasi — sebagaimana ditunjukkan oleh kontrol policy manifest dan compliance checker otomatis yang diterapkan secara konsisten pada VM2 maupun VM3.

5.3 Kesimpulan

1. Duplikasi lab CTF Amethysts sebagai VM1 berhasil menyediakan baseline vulnerable machine yang merepresentasikan kondisi sistem tanpa kontrol keamanan, dengan seluruh 13 tahap attack chain dapat direproduksi secara konsisten.
2. Penerapan kontrol Zero Trust dengan pendekatan Detect-First pada VM2 berhasil meningkatkan visibilitas serangan dari 0% menjadi 100%, dengan satu kontrol kritis (inotify upload monitor) yang mampu memutus rantai serangan pada tahap #10 tanpa mengorbankan reproduktifitas tahap-tahap lainnya.
3. Penerapan kontrol Full Enforcement pada VM3 berhasil menurunkan tingkat keberhasilan serangan end-to-end secara signifikan, dari 92,3% (VM2) menjadi 23,1% (VM3), dengan attack chain terputus pada tahap #3 — jauh lebih dini dibandingkan VM2.
4. Pendekatan bertahap (Baseline → Detect-First → Full Enforcement) yang diterapkan pada penelitian ini terbukti efektif sebagai metodologi untuk mendemonstrasikan secara kuantitatif

dampak penerapan prinsip Zero Trust terhadap suatu attack chain nyata, sekaligus memvalidasi kesesuaiannya dengan pilar-pilar CISA ZTMM v2.0.

5.4 Saran Penelitian Lanjutan

- Menyelesaikan dan memverifikasi kontrol whitelist ekstensi unggah pada level aplikasi (admin.php) sebagai lapisan pertahanan ketiga pada VM3.
- Melakukan pengujian Jalur B (independent testing) secara menyeluruh untuk mengukur efektivitas masing-masing kontrol secara terpisah dari urutan attack chain asli.
- Mengeksplorasi penerapan Multi-Factor Authentication (MFA) sebagai pembanding terhadap kontrol SSH Key-Based Authentication yang telah diterapkan pada VM3.
- Memperluas cakupan pengujian pada topologi jaringan yang lebih kompleks (non-flat network) untuk mengevaluasi kontrol berbasis segmentasi IP yang sebelumnya dinyatakan tidak applicable pada penelitian ini.

LAMPIRAN — CATATAN TROUBLESHOOTING

Lampiran ini mendokumentasikan proses debugging yang terpisah dari langkah-langkah final pada Bab III dan Bab IV, disajikan sebagai bagian dari dokumentasi metodologis proses implementasi.

Lampiran A — Troubleshooting Implementasi VM2 (Bab III)

A.1 Log Kernel nftables Tidak Masuk ke ZT Log (Sesi 1)

Gejala: rule nftables aktif dan log tampak pada journalctl, namun /var/log/zerotrust/alerts.log tetap kosong. Investigasi menemukan dua akar masalah: (1) rule rsyslog berbasis filter pesan (:msg, contains) tidak cocok karena pesan kernel diproses lebih dulu oleh facility kern.* pada berkas 50-default.conf sebelum sempat dicocokkan oleh rule kustom; dan (2) proses rsyslog berjalan sebagai pengguna syslog namun berkas log dimiliki root:adm tanpa akses tulis grup yang sesuai. Perbaikan dilakukan dengan mengubah rule menjadi menangkap facility kern.* secara eksplisit, serta menyesuaikan kepemilikan berkas menjadi syslog:adm.

A.2 Format Log vsftpd Tidak Cocok dengan Script Monitor (Sesi 2)

Gejala: script zt-ftp-monitor.sh tidak menghasilkan alert meskipun nftables telah mencatat koneksi FTP. Penyebabnya, pola pencocokan awal mencari kata anonymous dan RETR, sedangkan format aktual output vsftpd (dengan log_ftp_protocol=YES) menggunakan pola OK LOGIN, OK DOWNLOAD, dan “LIST. Perbaikan dilakukan dengan menyesuaikan pola grep pada script.

A.3 Jail fail2ban SSH Gagal Dimuat (Sesi 3)

Gejala: fail2ban gagal memuat jail zt-ssh-brute karena merujuk pada filter dengan nama yang sama, padahal berkas filter khusus tersebut tidak pernah dibuat. Perbaikan dilakukan dengan mengarahkan parameter filter pada jail tersebut ke filter bawaan fail2ban yang sudah tersedia (filter = sshd).

A.4 Systemd Unit Gagal Dibuat Lewat Editor Interaktif (Sesi 5)

Gejala: sudo systemctl enable zt-audit-monitor menghasilkan error “‘multi-user.targety’ is not a valid unit name”. Penyebabnya, berkas service dibuat melalui nano secara interaktif dan proses tempel teks menyisipkan karakter tambahan pada baris WantedBy. Perbaikan dilakukan dengan membuat ulang berkas secara non-interaktif menggunakan heredoc bash, yang kemudian dijadikan standar untuk seluruh pembuatan berkas konfigurasi/service pada dokumentasi ini.

A.5 Compliance Checker: 3 dari 23 Kontrol Gagal (Sesi Policy)

Uji pertama menghasilkan 20/23 PASS (86%). Tiga kegagalan disebabkan oleh permission dan kepemilikan berkas .env yang belum diterapkan (baru berupa rencana pada policy manifest), serta rule auditd zt_device_vim_cap yang belum di-reload pasca perubahan sistem. Perbaikan diterapkan langsung dan diverifikasi ulang menggunakan compliance checker.

Lampiran B — Troubleshooting Penguatan VM2 dan Implementasi VM3 (Bab IV)

B.1 Rule auditd Hilang Setelah Reboot

Beberapa pendekatan dicoba untuk mengatasi hilangnya rule auditd pasca-reboot: penggunaan systemctl edit auditd untuk menambahkan drop-in override sempat gagal karena berkas override tidak tersimpan dengan benar, dan percobaan berikutnya menghasilkan berkas override kosong yang

menyebabkan auditd gagal start total. Solusi akhir yang dipilih adalah menghapus drop-in yang bermasalah, mengembalikan auditd ke kondisi default, dan menambahkan job cron @reboot yang menjalankan augenrules --load setelah jeda 5 detik.

B.2 Duplikasi Entri pada Data Inventory Script

Hasil scan awal menampilkan entri .env dan .env.enc secara duplikat karena direktori /var/www/Amethyst_Dev_2024 didaftarkan terpisah padahal sudah tercakup dalam /var/www. Selain itu, proof.txt tidak muncul karena direktori /root belum dimasukkan ke daftar scan. Perbaikan dilakukan dengan menyesuaikan daftar direktori scan menjadi /srv/ftp, /home/jossie, /var/www, dan /root.

B.3 fail2ban Tidak Mendeteksi Hydra pada VM3

Setelah threshold fail2ban diperketat, percobaan awal menunjukkan Total failed: 0 meskipun hydra telah dijalankan berulang kali. Diagnosis menemukan bahwa request hydra tercatat pada log akses umum dengan kode respons 503 (akibat rate limiting nginx), bukan pada log admin yang dipantau fail2ban, dan pola filter yang digunakan juga tidak mencocokkan kode respons tersebut. Perbaikan dilakukan dengan menyesuaikan logpath dan pola failregex pada filter fail2ban.

B.4 Verifikasi PHP disable_functions Tidak Terbaca via CLI

Perintah verifikasi awal menggunakan konteks PHP CLI, yang terpisah dari konfigurasi PHP-FPM tempat berkas hardening disimpan, sehingga hasil verifikasi tampak kosong. Perbaikan dilakukan dengan menunjuk secara eksplisit berkas konfigurasi FPM melalui argumen -c saat verifikasi.

B.5 setcap -r Gagal karena Binary vim Masih Immutable

Perintah penghapusan capability pada VM3 gagal karena binary vim masih memiliki atribut immutable yang dipasang pada VM2 dan ikut terbawa saat proses cloning. Perbaikan dilakukan dengan melepas atribut immutable (chattr -i) terlebih dahulu sebelum capability dapat dihapus. Sebagai konsekuensinya, pemeriksaan “vim binary immutable” pada compliance checker VM2 digantikan dengan pemeriksaan “vim capability dihapus” pada compliance checker VM3, karena kedua kontrol tersebut saling eksklusif.

B.6 PasswordAuthentication no Tidak Efektif

Meskipun sshd_config telah diatur ke PasswordAuthentication no, login menggunakan password tetap berhasil. Diagnosis bertahap menemukan dua penyebab: pengaturan UsePAM yes yang dapat mengoverride pengaturan password authentication, serta berkas drop-in otomatis dari cloud-init (/etc/ssh/sshd_config.d/50-cloud-init.conf) yang berisi PasswordAuthentication yes dan diproses setelah konfigurasi utama sehingga mengoverride-nya. Perbaikan dilakukan dengan menambahkan UsePAM no dan menimpa berkas drop-in cloud-init tersebut secara eksplisit.

B.7 Compliance Checker VM3 — 2 Kegagalan pada Uji Pertama

Uji pertama menghasilkan 29/31 PASS. Dua kegagalan disebabkan oleh checker yang masih mewarisi nilai pemeriksaan dari VM2 (MaxAuthTries=6, padahal VM3 menggunakan nilai 3), serta pemeriksaan “vim binary immutable” yang otomatis gagal karena atribut tersebut memang sengaja dilepas pada VM3. Setelah penyesuaian checker, hasil akhir menjadi 30/30 PASS (100%).