LAMPIRAN

Lampiran 1. Proses Konfigurasi Manual yang Dilakukan Administrator

No	Proses Manual	Aktivitas Administrator	Hasil yang Diharapkan
1	Login ke MikroTik	Administrator membuka aplikasi Winbox kemudian login ke router menggunakan akun administrator.	Berhasil masuk ke halaman konfigurasi RouterOS.
2	Memeriksa Address List	Membuka menu IP → Firewall → Address Lists, kemudian memeriksa apakah terdapat alamat IP yang masuk ke suspicious_ip.	IP penyerang berhasil teridentifikasi pada address list suspicious_ip.
3	Memasukkan IP ke *Blacklist*	Menyalin alamat IP dari suspicious_ip, kemudian menambahkan IP tersebut secara manual ke address list *blacklist*.	IP berhasil masuk ke address list *blacklist* sehingga diblokir oleh firewall.
4	Mengubah Rule Port Knocking 1	Membuka menu IP → Firewall → Filter Rules, mencari rule Knock 1, kemudian mengubah nilai *Destination port* (*dst-port*) sesuai port baru yang diinginkan.	Rule Knock 1 menggunakan port baru.
5	Mengubah Rule Port Knocking 2	Mencari rule Knock 2, kemudian mengubah nilai *Destination port* (*dst-port*).	Rule Knock 2 menggunakan port baru.
6	Mengubah Rule Port Knocking 3	Mencari rule Knock 3, kemudian mengubah nilai *Destination port* (*dst-port*).	Rule Knock 3 menggunakan port baru.
7	Menyimpan Perubahan	Menekan tombol Apply dan OK pada setiap rule yang telah dimodifikasi.	Seluruh perubahan konfigurasi tersimpan pada RouterOS.

Lampiran 2. Hasil Pengujian dengan 3 Attacker dan 60 detik interval

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

	Name	Address	Timeout	Creation Time
	;;; EDA-AutoBlock			
D	blacklist	192.168.10.2	23:59:55	Jul/13/2026 23:58:37
	;;; EDA-AutoBlock			
D	blacklist	192.168.10.3	23:59:57	Jul/13/2026 23:58:38
	;;; EDA-AutoBlock			
D	blacklist	192.168.10.4	23:59:58	Jul/13/2026 23:58:40
	ip_whitelist	10.10.10.10		May/25/2026 01:21:04
D	stage1	192.168.10.2	00:00:23	Jul/13/2026 23:57:54
D	stage1	192.168.10.3	00:00:17	Jul/13/2026 23:57:59
D	stage1	192.168.10.4	00:00:27	Jul/13/2026 23:57:59
D	stage2	192.168.10.2	00:00:23	Jul/13/2026 23:57:54
D	stage2	192.168.10.3	00:00:18	Jul/13/2026 23:57:59
D	stage2	192.168.10.4	00:00:19	Jul/13/2026 23:58:00
D	stage3	192.168.10.2	00:00:23	Jul/13/2026 23:57:54
D	stage3	192.168.10.3	00:00:18	Jul/13/2026 23:57:59
D	stage3	192.168.10.4	00:00:19	Jul/13/2026 23:58:00
D	suspicious_ip	192.168.10.2	00:00:53	Jul/13/2026 23:57:54
D	suspicious_ip	192.168.10.3	00:00:48	Jul/13/2026 23:57:59
D	suspicious_ip	192.168.10.4	00:00:49	Jul/13/2026 23:58:00
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.10.2	00:00:43	Jul/13/2026 23:58:33
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.10.3	00:00:48	Jul/13/2026 23:58:34
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.10.4	00:00:49	Jul/13/2026 23:58:35

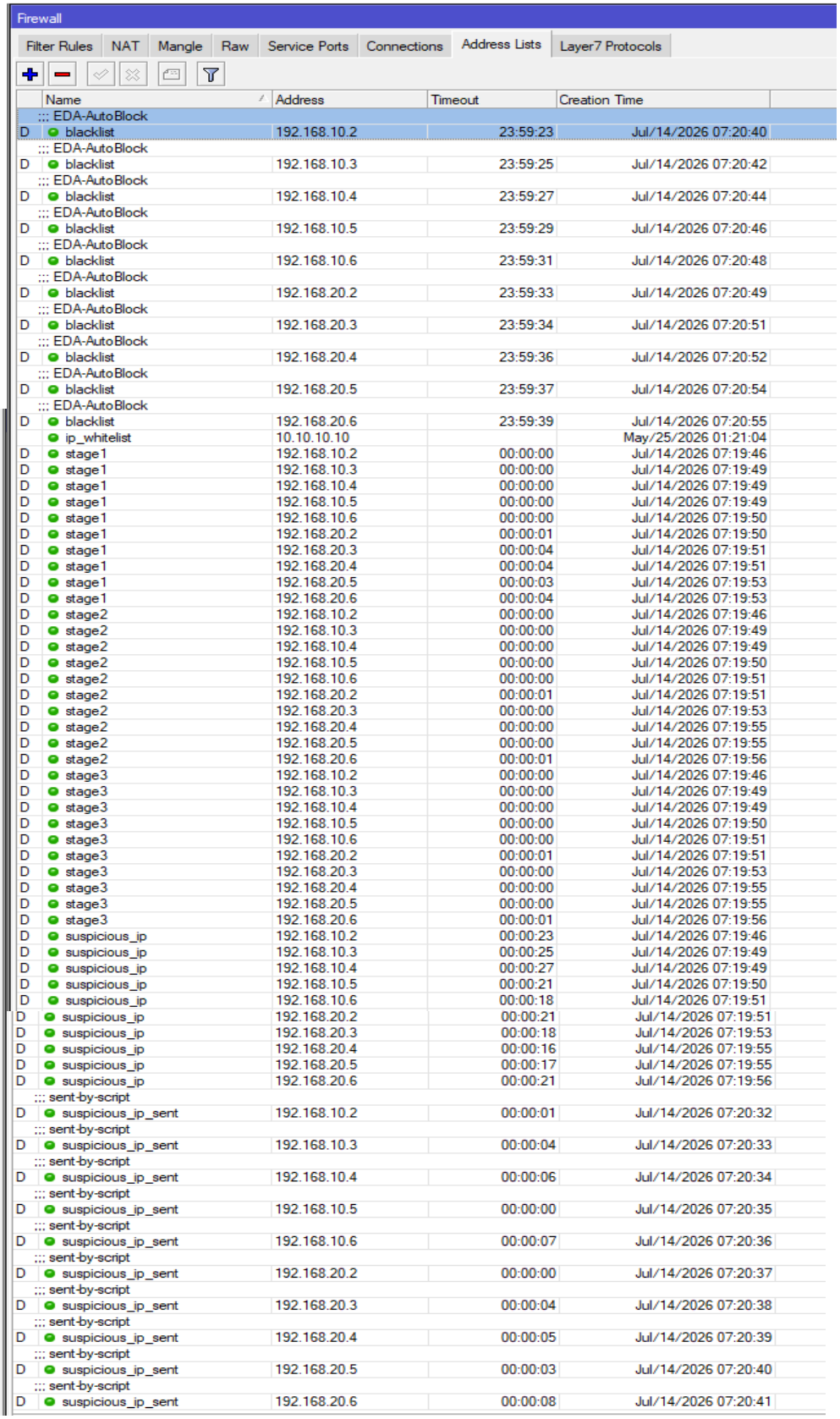
Lampiran 3. Hasil Pengujian dengan 5 Attacker dan 60 detik interval

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

	Name	Address	Timeout	Creation Time
	;;; EDA-AutoBlock			
D	blacklist	192.168.10.2	23:59:47	Jul/14/2026 00:09:38
	;;; EDA-AutoBlock			
D	blacklist	192.168.10.3	23:59:49	Jul/14/2026 00:09:40
	;;; EDA-AutoBlock			
D	blacklist	192.168.10.4	23:59:51	Jul/14/2026 00:09:41
	;;; EDA-AutoBlock			
D	blacklist	192.168.10.5	23:59:52	Jul/14/2026 00:09:43
	;;; EDA-AutoBlock			
D	blacklist	192.168.10.6	23:59:54	Jul/14/2026 00:09:45
	ip_whitelist	10.10.10.10		May/25/2026 01:21:04
D	stage1	192.168.10.2	00:00:11	Jul/14/2026 00:08:50
D	stage1	192.168.10.3	00:00:17	Jul/14/2026 00:08:53
D	stage1	192.168.10.4	00:00:16	Jul/14/2026 00:08:53
D	stage1	192.168.10.5	00:00:15	Jul/14/2026 00:08:53
D	stage1	192.168.10.6	00:00:15	Jul/14/2026 00:08:54
D	stage2	192.168.10.2	00:00:11	Jul/14/2026 00:08:50
D	stage2	192.168.10.3	00:00:17	Jul/14/2026 00:08:53
D	stage2	192.168.10.4	00:00:16	Jul/14/2026 00:08:54
D	stage2	192.168.10.5	00:00:17	Jul/14/2026 00:08:55
D	stage2	192.168.10.6	00:00:17	Jul/14/2026 00:08:55
D	stage3	192.168.10.2	00:00:11	Jul/14/2026 00:08:50
D	stage3	192.168.10.3	00:00:17	Jul/14/2026 00:08:53
D	stage3	192.168.10.4	00:00:16	Jul/14/2026 00:08:54
D	stage3	192.168.10.5	00:00:17	Jul/14/2026 00:08:55
D	stage3	192.168.10.6	00:00:17	Jul/14/2026 00:08:55
D	suspicious_ip	192.168.10.2	00:00:41	Jul/14/2026 00:08:50
D	suspicious_ip	192.168.10.3	00:00:47	Jul/14/2026 00:08:53
D	suspicious_ip	192.168.10.4	00:00:46	Jul/14/2026 00:08:54
D	suspicious_ip	192.168.10.5	00:00:47	Jul/14/2026 00:08:55
D	suspicious_ip	192.168.10.6	00:00:47	Jul/14/2026 00:08:55
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.10.2	00:00:41	Jul/14/2026 00:09:33
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.10.3	00:00:36	Jul/14/2026 00:09:34
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.10.4	00:00:34	Jul/14/2026 00:09:35
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.10.5	00:00:36	Jul/14/2026 00:09:36
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.10.6	00:00:36	Jul/14/2026 00:09:37

Lampiran 4. Hasil Pengujian dengan 10 Attacker dan 60 detik interval



Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

	Name	Address	Timeout	Creation Time
	;;; EDA-AutoBlock			
D	blacklist	192.168.10.2	23:59:23	Jul/14/2026 07:20:40
	;;; EDA-AutoBlock			
D	blacklist	192.168.10.3	23:59:25	Jul/14/2026 07:20:42
	;;; EDA-AutoBlock			
D	blacklist	192.168.10.4	23:59:27	Jul/14/2026 07:20:44
	;;; EDA-AutoBlock			
D	blacklist	192.168.10.5	23:59:29	Jul/14/2026 07:20:46
	;;; EDA-AutoBlock			
D	blacklist	192.168.10.6	23:59:31	Jul/14/2026 07:20:48
	;;; EDA-AutoBlock			
D	blacklist	192.168.20.2	23:59:33	Jul/14/2026 07:20:49
	;;; EDA-AutoBlock			
D	blacklist	192.168.20.3	23:59:34	Jul/14/2026 07:20:51
	;;; EDA-AutoBlock			
D	blacklist	192.168.20.4	23:59:36	Jul/14/2026 07:20:52
	;;; EDA-AutoBlock			
D	blacklist	192.168.20.5	23:59:37	Jul/14/2026 07:20:54
	;;; EDA-AutoBlock			
D	blacklist	192.168.20.6	23:59:39	Jul/14/2026 07:20:55
	ip_whitelist	10.10.10.10		May/25/2026 01:21:04
D	stage1	192.168.10.2	00:00:00	Jul/14/2026 07:19:46
D	stage1	192.168.10.3	00:00:00	Jul/14/2026 07:19:49
D	stage1	192.168.10.4	00:00:00	Jul/14/2026 07:19:49
D	stage1	192.168.10.5	00:00:00	Jul/14/2026 07:19:49
D	stage1	192.168.10.6	00:00:00	Jul/14/2026 07:19:50
D	stage1	192.168.20.2	00:00:01	Jul/14/2026 07:19:50
D	stage1	192.168.20.3	00:00:04	Jul/14/2026 07:19:51
D	stage1	192.168.20.4	00:00:04	Jul/14/2026 07:19:51
D	stage1	192.168.20.5	00:00:03	Jul/14/2026 07:19:53
D	stage1	192.168.20.6	00:00:04	Jul/14/2026 07:19:53
D	stage2	192.168.10.2	00:00:00	Jul/14/2026 07:19:46
D	stage2	192.168.10.3	00:00:00	Jul/14/2026 07:19:49
D	stage2	192.168.10.4	00:00:00	Jul/14/2026 07:19:49
D	stage2	192.168.10.5	00:00:00	Jul/14/2026 07:19:50
D	stage2	192.168.10.6	00:00:00	Jul/14/2026 07:19:51
D	stage2	192.168.20.2	00:00:01	Jul/14/2026 07:19:51
D	stage2	192.168.20.3	00:00:00	Jul/14/2026 07:19:53
D	stage2	192.168.20.4	00:00:00	Jul/14/2026 07:19:55
D	stage2	192.168.20.5	00:00:00	Jul/14/2026 07:19:55
D	stage2	192.168.20.6	00:00:01	Jul/14/2026 07:19:56
D	stage3	192.168.10.2	00:00:00	Jul/14/2026 07:19:46
D	stage3	192.168.10.3	00:00:00	Jul/14/2026 07:19:49
D	stage3	192.168.10.4	00:00:00	Jul/14/2026 07:19:49
D	stage3	192.168.10.5	00:00:00	Jul/14/2026 07:19:50
D	stage3	192.168.10.6	00:00:00	Jul/14/2026 07:19:51
D	stage3	192.168.20.2	00:00:01	Jul/14/2026 07:19:51
D	stage3	192.168.20.3	00:00:00	Jul/14/2026 07:19:53
D	stage3	192.168.20.4	00:00:00	Jul/14/2026 07:19:55
D	stage3	192.168.20.5	00:00:00	Jul/14/2026 07:19:55
D	stage3	192.168.20.6	00:00:01	Jul/14/2026 07:19:56
D	suspicious_ip	192.168.10.2	00:00:23	Jul/14/2026 07:19:46
D	suspicious_ip	192.168.10.3	00:00:25	Jul/14/2026 07:19:49
D	suspicious_ip	192.168.10.4	00:00:27	Jul/14/2026 07:19:49
D	suspicious_ip	192.168.10.5	00:00:21	Jul/14/2026 07:19:50
D	suspicious_ip	192.168.10.6	00:00:18	Jul/14/2026 07:19:51
D	suspicious_ip	192.168.20.2	00:00:21	Jul/14/2026 07:19:51
D	suspicious_ip	192.168.20.3	00:00:18	Jul/14/2026 07:19:53
D	suspicious_ip	192.168.20.4	00:00:16	Jul/14/2026 07:19:55
D	suspicious_ip	192.168.20.5	00:00:17	Jul/14/2026 07:19:55
D	suspicious_ip	192.168.20.6	00:00:21	Jul/14/2026 07:19:56
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.10.2	00:00:01	Jul/14/2026 07:20:32
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.10.3	00:00:04	Jul/14/2026 07:20:33
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.10.4	00:00:06	Jul/14/2026 07:20:34
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.10.5	00:00:00	Jul/14/2026 07:20:35
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.10.6	00:00:07	Jul/14/2026 07:20:36
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.20.2	00:00:00	Jul/14/2026 07:20:37
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.20.3	00:00:04	Jul/14/2026 07:20:38
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.20.4	00:00:05	Jul/14/2026 07:20:39
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.20.5	00:00:03	Jul/14/2026 07:20:40
	;;; sent-by-script			
D	suspicious_ip_sent	192.168.20.6	00:00:08	Jul/14/2026 07:20:41

Lampiran 5. Kode Webhook

```
from flask import Flask, request, jsonify
import requests

app = Flask(__name__)

# Endpoint EDA (Ansible Rulebook)
EDA_URL = "http://127.0.0.1:5001"

@app.route('/ssh-blacklist', methods=['POST'])
def ssh_blacklist():
    print("\n=== REQUEST MASUK ===")

    # Debug raw input
    print("RAW DATA:", request.data)
    print("FORM:", request.form)
    print("JSON:", request.get_json(silent=True))

    # Ambil dari form (sesuai MikroTik kirim)
    data = request.form

    router = data.get("router")
    ip = data.get("attacker_ip")

    print("=== HASIL PARSE ===")
    print("Router :", router)
    print("IP     :", ip)
    print("====================")

    # Validasi sederhana
    if not router or not ip:
        return jsonify({
            "status": "error",
            "message": "router / attacker_ip missing"
        }), 400

    # Forward ke Ansible EDA (pakai JSON)
    payload = {
        "router": router,
        "attacker_ip": ip
    }

    try:
        response = requests.post(EDA_URL, json=payload,
timeout=5)

        print("=== FORWARD KE EDA ===")
        print("Status :", response.status_code)
        print("Resp   :", response.text)
        print("======================")

        return jsonify({
            "status": "forwarded",
            "eda_status": response.status_code
        })

    except requests.exceptions.RequestException as e:
        print("ERROR forward ke EDA:", str(e))
```

```
        return jsonify({
            "status": "error",
            "message": "gagal kirim ke EDA",
            "error": str(e)
        }), 500


if __name__ == "__main__":
    app.run(host="0.0.0.0", port=5000)
```

Lampiran 6. Kode inventory.yml

```
---
all:
  children:
    mikrotik:
      hosts:
        router1:
          ansible_host: 10.10.10.9
        router2:
          ansible_host: 10.10.10.2
        router3:
          ansible_host: 10.10.10.6
      vars:
        ansible_user: admin+e
        ansible_password: admin
        ansible_port: 22
        ansible_connection: ssh
        ansible_ssh_common_args: '-o StrictHostKeyChecking=no -o
UserKnownHostsFile=/dev/null -o
PreferredAuthentications=password -o PubkeyAuthentication=no'
```

Lampiran 7. Kode rulebook.yml

```
---
- name: Auto-Block Brute Force dari MikroTik
  hosts: all
  sources:
    - ansible.eda.webhook:
        host: 127.0.0.1
        port: 5001

  rules:

    - name: Block attacker IP dari MikroTik
      condition: >
        event.payload.attacker_ip is defined and
        event.payload.router is defined
      action:
```

```
        run_playbook:
          name: playbooks/block_ip.yml
          extra_vars:
            attacker_ip: "{{ event.payload.attacker_ip }}"
            router: "{{ event.payload.router }}"
```

Lampiran 8. Kode playbook.yml

```
---
- name: Block Attacker IP & Rotasi Port Knocking di MikroTik
  hosts: "{{ router }}"
  gather_facts: false
  vars:
    port_min: 10000
    port_max: 60000
    rotate_window: 60
    rotate_flag: "/tmp/eda_rotated_{{ router | replace('.', '_')
}}"

    # Komentar rule di MikroTik
    knock1_comment: "9 Knock1"
    knock2_comment: "10 Knock2"
    knock3_comment: "11 Knock3"

  tasks:
    # ============================================================
    # FASE 1: PROSES LOGIKA LOKAL (Sangat Cepat / Instan)
    # ============================================================
    - name: Cek rotate flag
      ansible.builtin.shell: |
        flag="{{ rotate_flag }}"
        now=$(date +%s)
        if [ -f "$flag" ]; then
          last=$(cat "$flag")
          diff=$((now - last))
          if [ $diff -lt {{ rotate_window }} ]; then
            echo "SKIP"
            exit 0
          fi
        fi
        echo "DO_ROTATE"
        echo "$now" > "$flag"
      delegate_to: localhost
      register: rotate_check
      changed_when: false

    - name: Set flag apakah perlu rotate
      set_fact:
        should_rotate: "{{ 'DO_ROTATE' in rotate_check.stdout
}}"

    - name: Generate port random untuk knock1
      set_fact:
        new_knock1: "{{ range(port_min, port_max + 1) | random
}}"
      delegate_to: localhost
      run_once: true
      when: should_rotate
```

```
    - name: Generate port random untuk knock2 (unik dari knock1)
      set_fact:
        new_knock2: "{{ range(port_min, port_max + 1) | random
}}"
      delegate_to: localhost
      run_once: true
      until: new_knock2 | int != new_knock1 | int
      retries: 20
      delay: 0
      when: should_rotate

    - name: Generate port random untuk knock3 (unik dari knock1
& knock2)
      set_fact:
        new_knock3: "{{ range(port_min, port_max + 1) | random
}}"
      delegate_to: localhost
      run_once: true
      until: >
        new_knock3 | int != new_knock1 | int and
        new_knock3 | int != new_knock2 | int
      retries: 20
      delay: 0
      when: should_rotate

    # ============================================================
    # FASE 2: PERSIAPAN COMMAND (Digabung dengan semicolon ;)
    # ============================================================
    - name: "Siapkan perintah dalam satu baris (Single Shot)"
      set_fact:
        mikrotik_final_cmd: >-
          /ip firewall address-list add list=blacklist
address={{ attacker_ip }} comment="EDA-AutoBlock" timeout=24h
          {% if should_rotate %}
          ; /ip firewall filter set [find comment="{{
knock1_comment }}"] dst-port={{ new_knock1 }}
          ; /ip firewall filter set [find comment="{{
knock2_comment }}"] dst-port={{ new_knock2 }}
          ; /ip firewall filter set [find comment="{{
knock3_comment }}"] dst-port={{ new_knock3 }}
          {% endif %}
          ; /quit

    # ============================================================
    # FASE 3: EKSEKUSI RAW SSH (Bypass Semua Pengecekan)
    # ============================================================
    - name: "Eksekusi Secepat Kilat (Raw SSH)"
      ansible.builtin.raw: "{{ mikrotik_final_cmd }}"
      changed_when: true

    # ============================================================
    # FASE 4: PELAPORAN
    # ============================================================
    - name: Summary — dengan rotasi
      debug:
        msg:
          - "SUKSES: {{ attacker_ip }} diblokir di {{ router }}"
          - "Port Knocking dirotasi:"
          - "  Knock1 : {{ new_knock1 }}"
```

```
          - "  Knock2 : {{ new_knock2 }}"
          - "  Knock3 : {{ new_knock3 }}"
          - "Urutan baru: {{ new_knock1 }} → {{ new_knock2 }} →
{{ new_knock3 }}"
      when: should_rotate

    - name: Summary — tanpa rotasi
      debug:
        msg:
          - "SUKSES: {{ attacker_ip }} diblokir di {{ router }}"
          - "Rotasi dilewati (sudah dirotasi dalam {{
rotate_window }} detik terakhir)"
      when: not should_rotate
```

Lampiran 9. Riwayat Hidup

RIWAYAT HIDUP

Andika Kurniawan Sianipar lahir pada 29 September 2004. Penulis berkebangsaan Indonesia dan beragama Kristen Protestan. Penulis tinggal di Kabupaten Deli Serdang. Penulis menempuh pendidikan sekolah dasar di SD Swasta Agia Sophia dan lulus pada tahun 2016. Jenjang menengah pertama penulis ditempuh di SMP Santo Yoseph Medan dan lulus pada tahun 2019. Jenjang menengah atas penulis ditempuh di SMk N 9 Medan dan diselesaikan pada tahun 2022. Penulis melanjutkan ke Strata 1 Jurusan Teknik Informatika di Universitas Pendidikan Ganesha pada tahun 2022. Pada semester akhir tahun 2026 penulis menyelesaikan Tugas Akhir yang berjudul "Otomatisasi Konfigurasi Port Blocking Dan Port Knocking Pada Perangkat Router Mikrotik Menggunakan Ansible". Tahun 2022 sampai dengan sekarang, penulis masih menjadi mahasiswa aktif di Program S1 Matematika Universitas Pendidikan Ganesha.