

Analizando ataques Slowloris com o **MENTORED** *Testbed*

Apresentadores:

- Michelle S. Wingham | UNIVALI/RNP
- Davi D. Gemmer | RNP



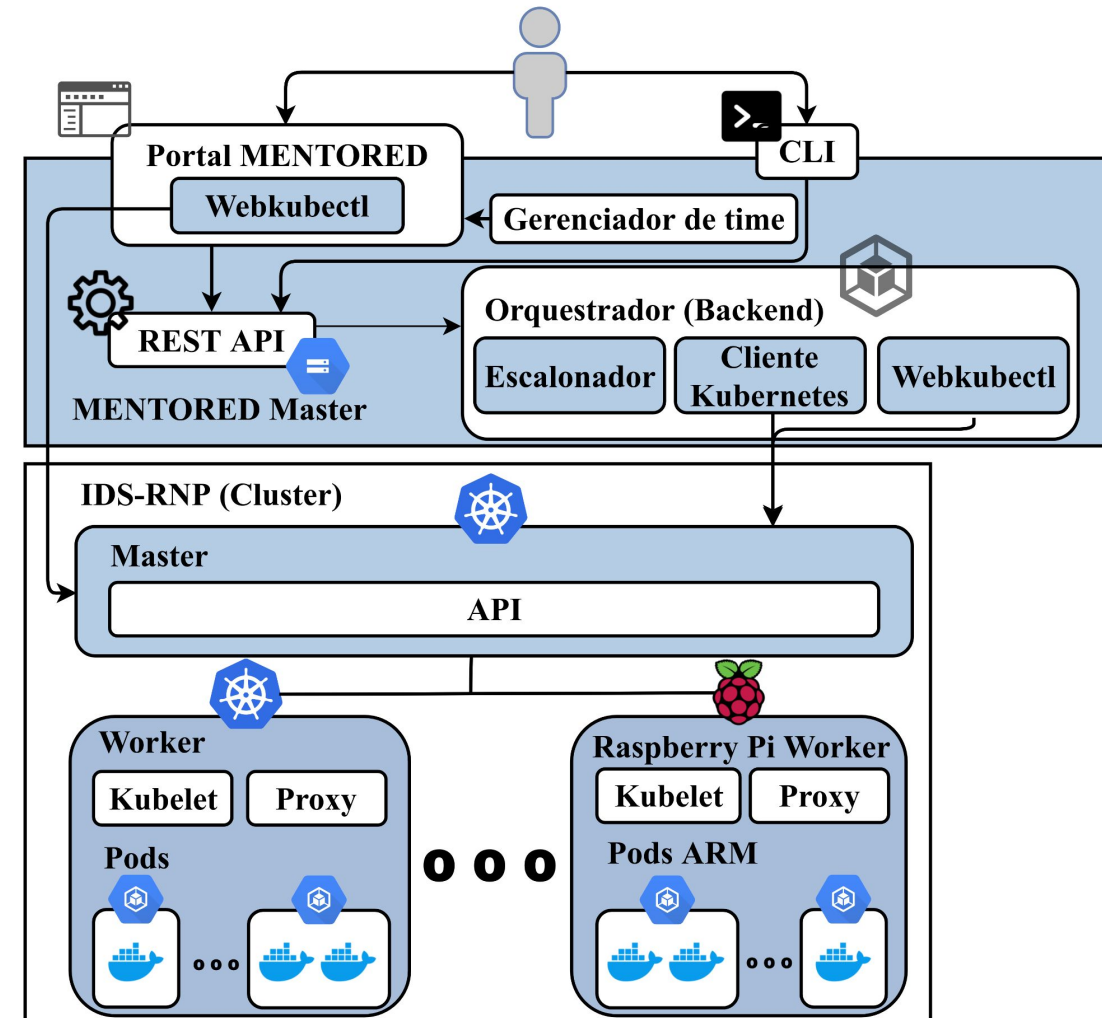
AGENDA

- **MENTORED *Testbed***
 - Arquitetura da implementação
 - Fluxo de execução de um experimento
- **Demonstração**
 - Características do ataque
 - Distribuição geográfica do ataque
 - Comportamento do ataque
 - Configuração do ataque
 - Execução do ataque
 - Resultados dos ataques

MENTORED *Testbed*

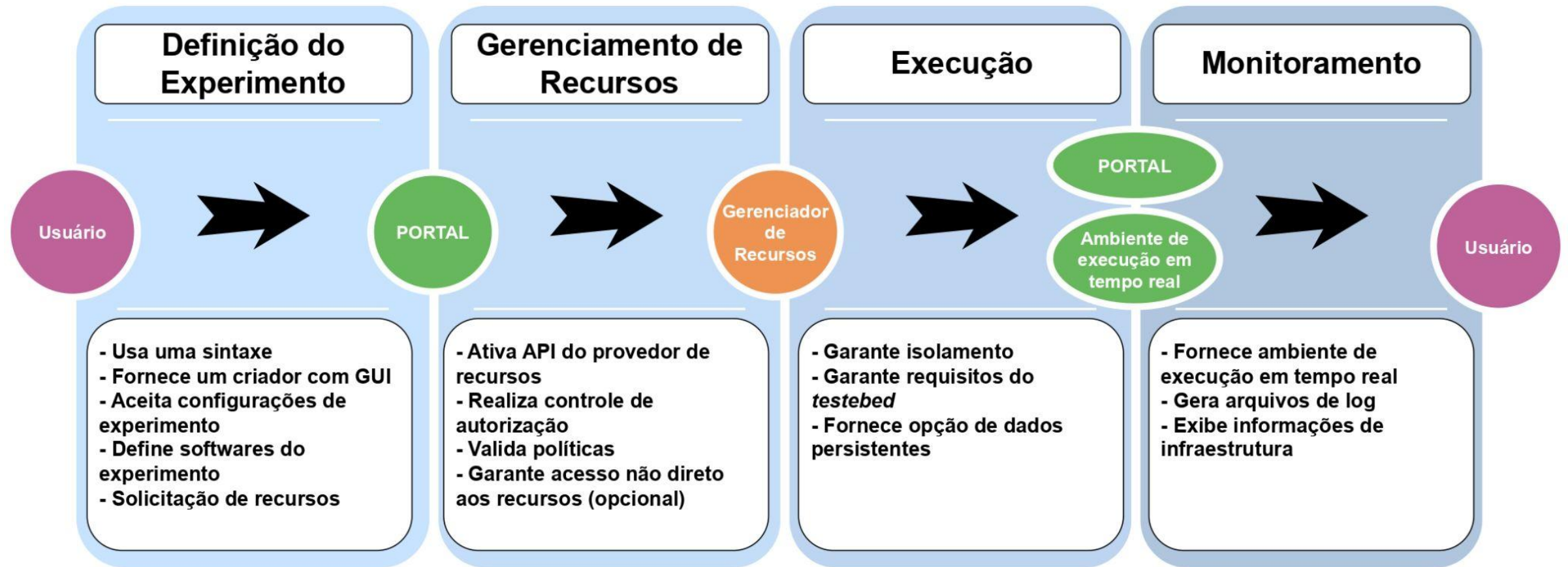
Arquitetura da implementação

- Principais tecnologias:
 - Kubernetes (cluster)
 - WebKubectl (**Terminal no browser**)
 - React (**Portal**)
 - Django REST (**API**)
 - COnmanage (Gerenciador de time)
- Desafios
 - Cluster é dinâmico
 - Múltiplos experimentadores
 - Recursos finitos**



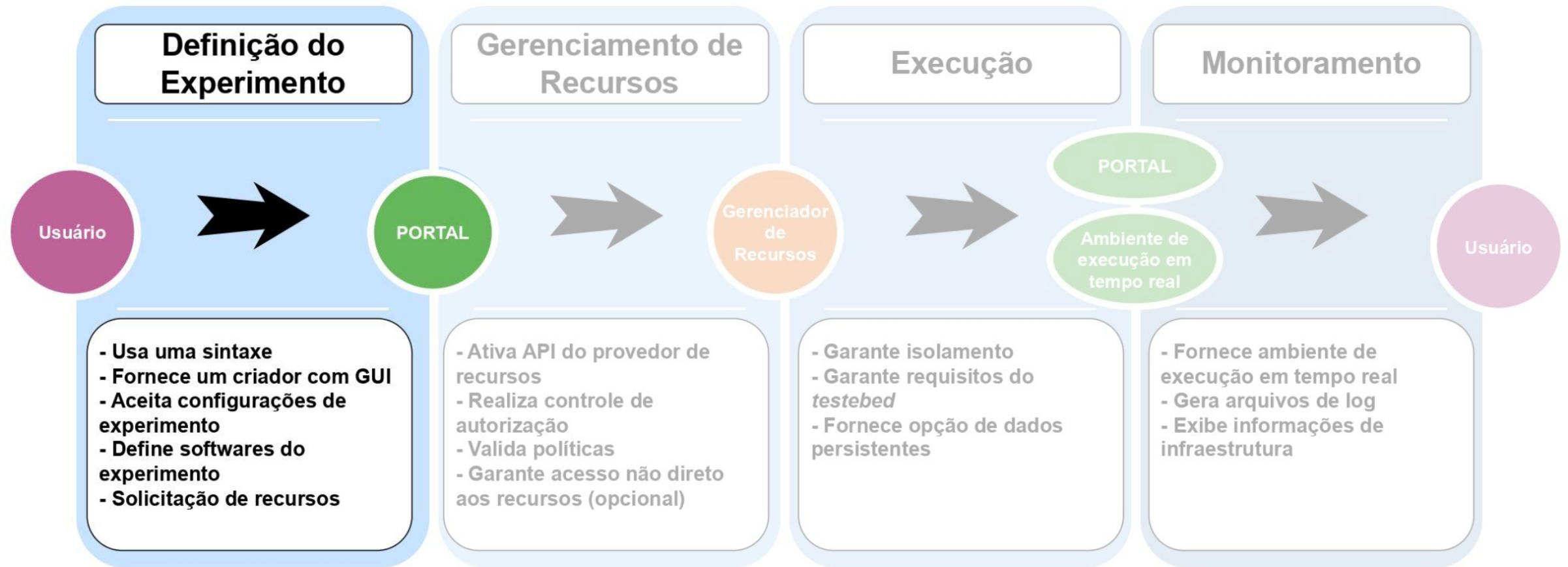
MENTORED *Testbed*

Fluxo de execução de experimento



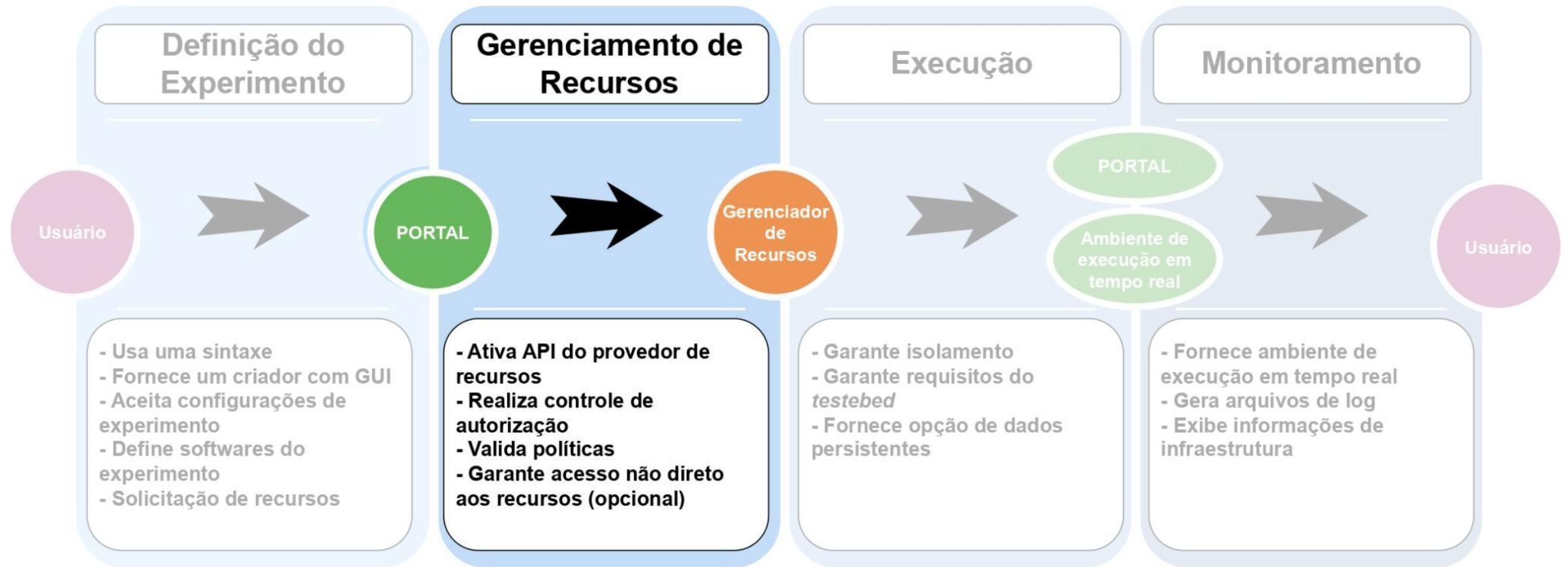
MENTORED *Testbed*

Definição do experimento



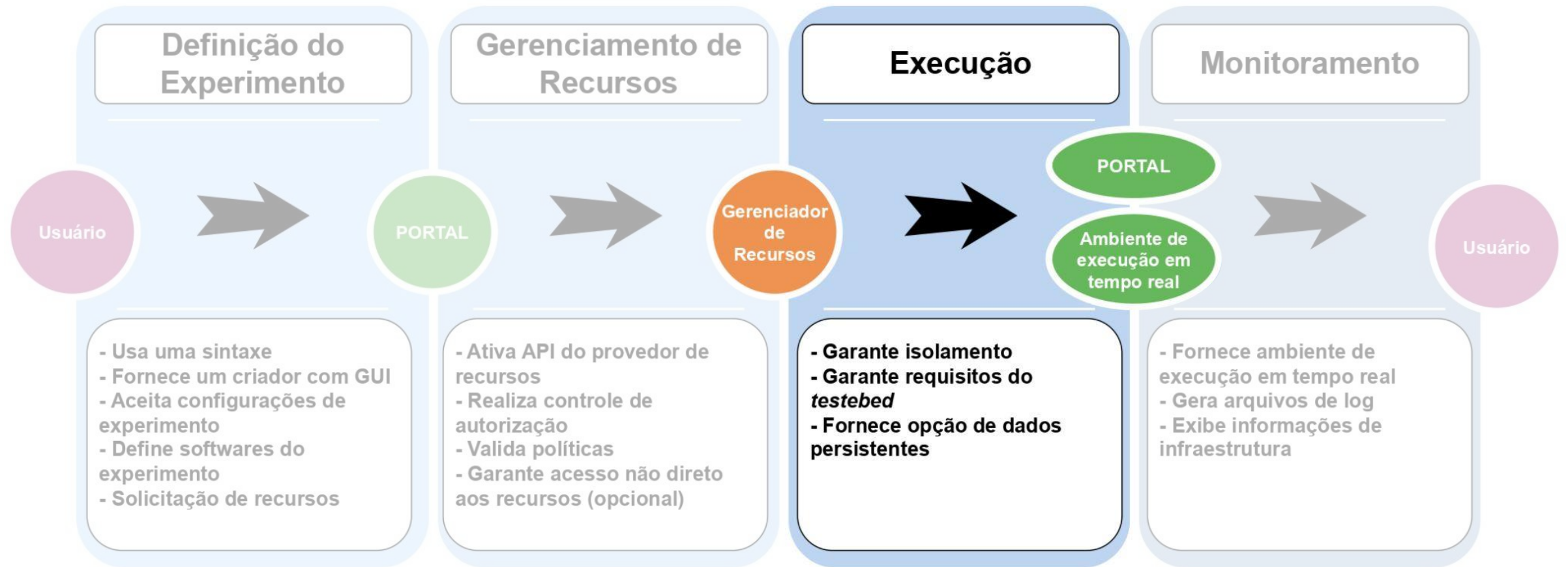
MENTORED *Testbed*

Gerenciamento de recursos



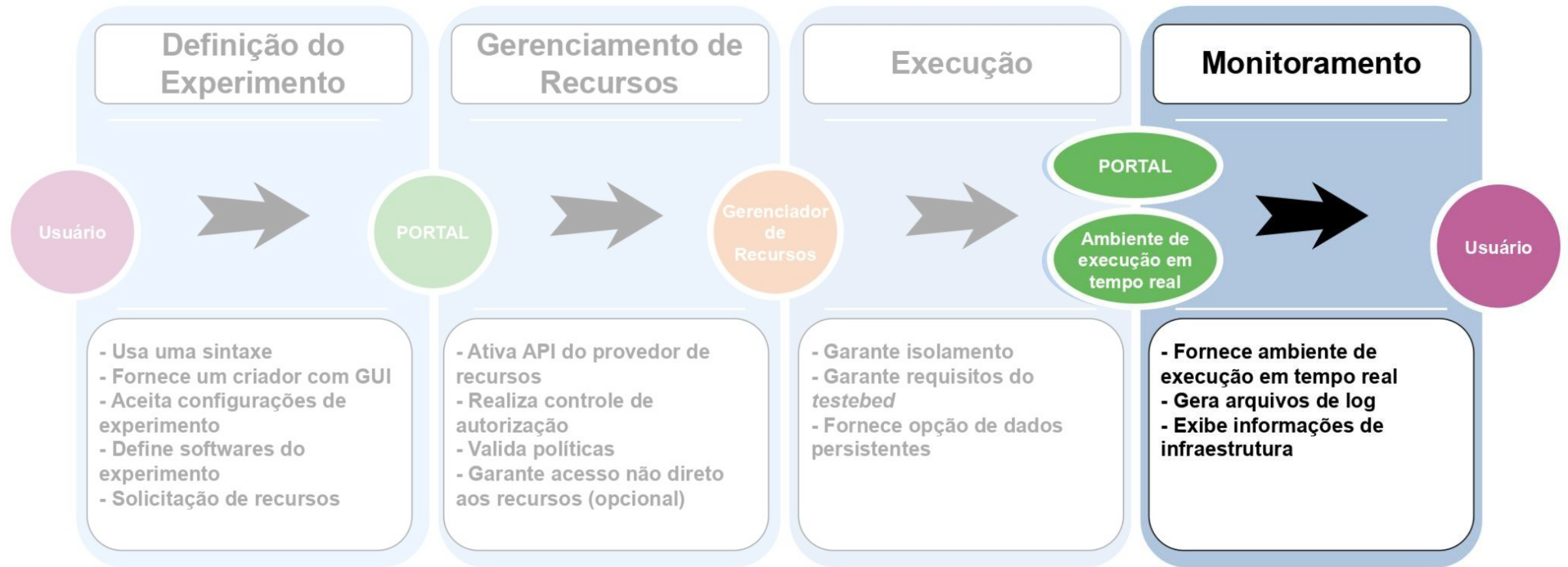
MENTORED *Testbed*

Execução



MENTORED *Testbed*

Monitoramento



Demonstração

Demonstração

Ataque Slowloris

- *Um ataque "low and slow" é um tipo de ataque DoS ou DDoS que depende de um pequeno streaming de tráfego muito lento visando recursos de aplicativos ou servidores;*
- *Layer 7 - Aplicações como servidores Web;*
- *Baixo consumo de rede.*

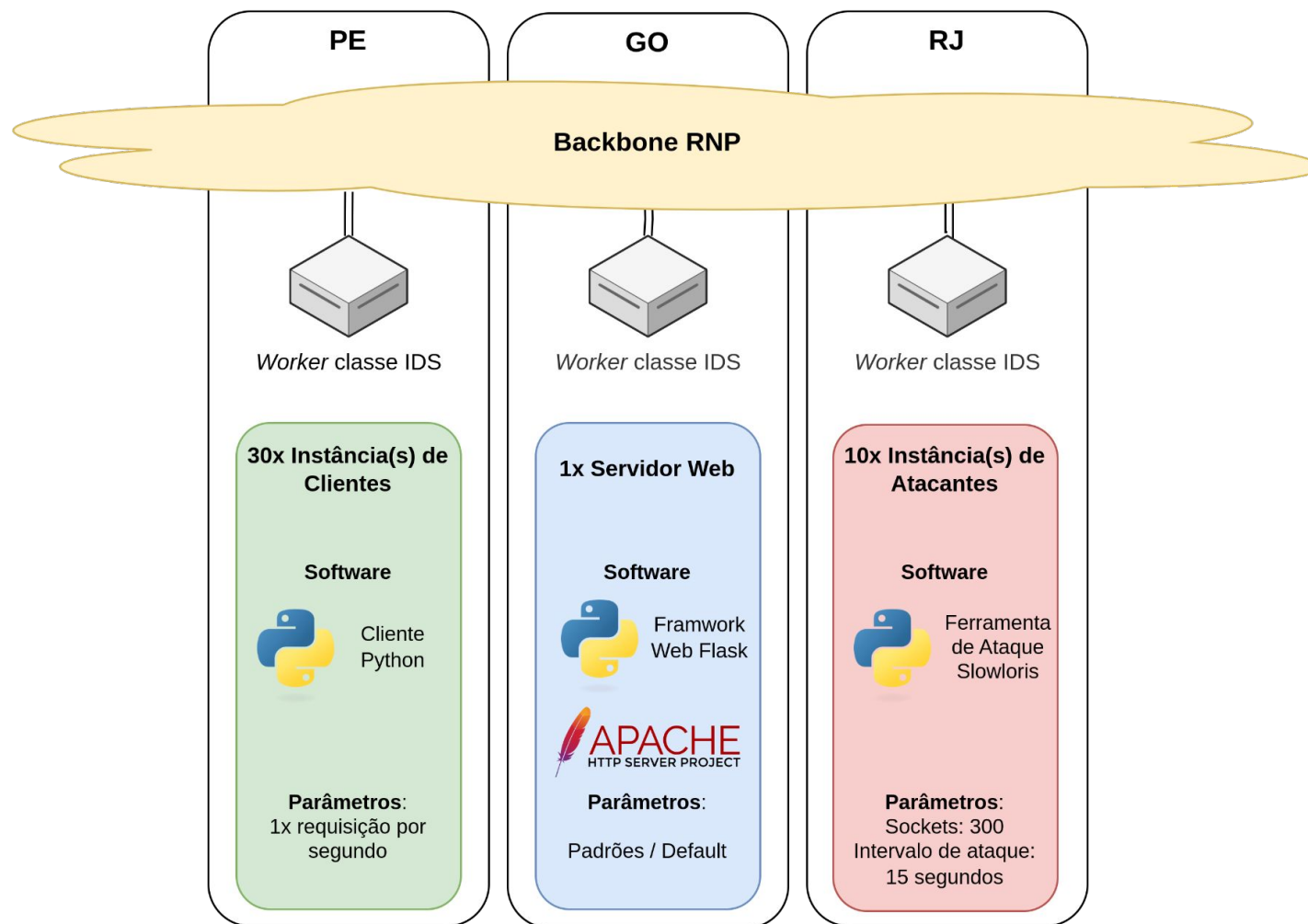
Demonstração

Configuração do servidor Web

- Ataque nº 1
 - Ataque Slowloris com servidor Apache2 *default*
 - Versão **default** do Apache2
- Ataque nº 2
 - Ataque Slowloris com servidor Apache2 modificado
 - Ativação do módulo **mod_reqtimeout** no código do Apache2.

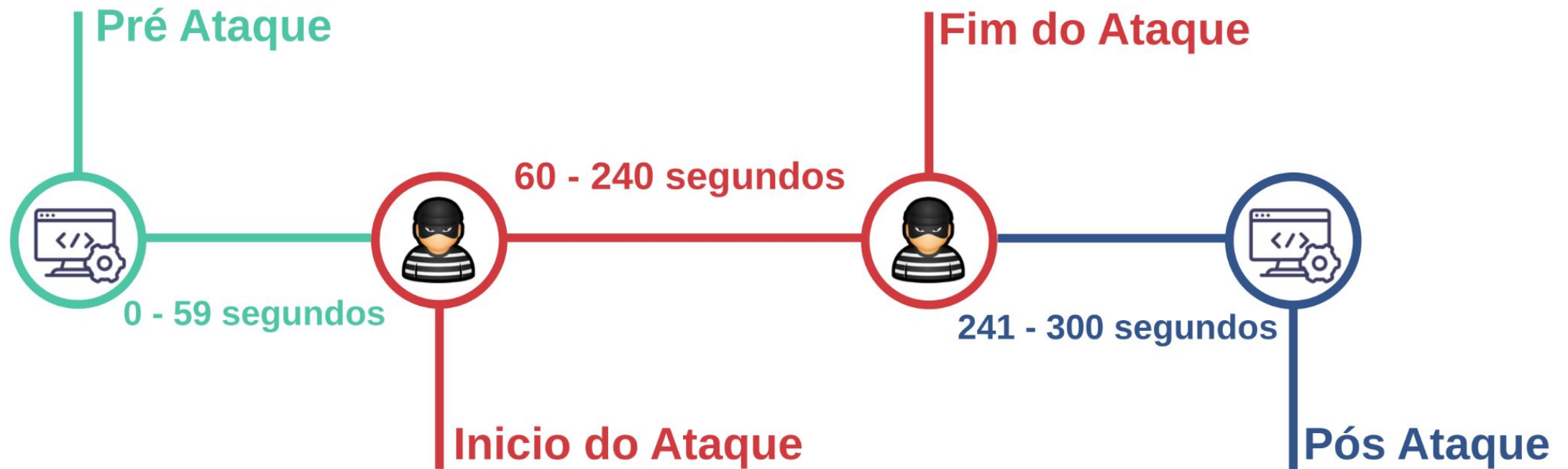
Demonstração

Configuração do ataque com Slowloris



Experimentos

Comportamento do ataque



Vítima - Ataque nº 1

Parte do código responsável pelo servidor

```
1 Experiment:
2   name: mentored_experiment
3   nodeactors:
4     - name: 'na-server'
5       persitent_volume_path: "/app/packets.pcap"
6       replicas: 1
7       containers:
8         - name: tshark
9           image: ghcr.io/mentoredtestbed/mentored-tshark
10          command: ["/entry.sh"]
11          args: ["tshark", "-i", "net1", "-x", "-w", "packets.pcap"]
12          env:
13            - name: TIMEOUT_CMD
14              value: "300"
15        - name: 'server'
16          image: ghcr.io/mentoredtestbed/generic-apache-flask-webserver:latest
17          ports:
18            - containerPort: 80
19          resources:
20            requests:
21              memory: 1G
22              cpu: "1"
23            limits:
24              memory: "2G"
25              cpu: "2"
26          region: 'ids-go'
```


Clientes

Parte do código responsável pelos clientes

```
1  - name: 'generic-client-pe'
2    persitent_volume_path: "/client_delay.csv"
3    replicas: 30
4    containers:
5      - name: 'client-rn'
6        image: ghcr.io/mentoredtestbed/generic-client:latest
7        imagePullPolicy: "Always"
8        command: ["/entry.sh"]
9        args: ['python3', 'client_web_metrics.py', "1", "1"]
10       env:
11         - name: TIMEOUT_CMD
12           value: "300"
13         - name: ADD_SERVER_IP_TO_COMMAND
14           value: "true"
15       resources:
16         requests:
17           memory: "64Mi"
18           cpu: "100m"
19         limits:
20           memory: "128M"
21           cpu: "200m"
22     region: 'ids-pe'
```

Atacante

Parte do código responsável pelos atacantes

```
1   - name: 'generic-botnet-rj'
2     persitent_volume_path: "/MENTORED_IP_LIST.yaml"
3     replicas: 10
4     containers:
5       - name: 'botnet-rn'
6         image: ghcr.io/mentoredtestbed/generic-botnet:latest
7         command: ["/entry.sh"]
8         args: ["slowloris", "-p", "80", "--randuseragents", "-s", "300"]
9         # args: ["hping3", "-S", "--flood", "-S", "-d 1024", "-p", "80"]
10        env:
11          - name: PROTOCOL
12            value: "ICMP"
13          - name: TIMEOUT_CMD
14            value: "180"
15          - name: TIME_WAIT_START
16            value: "60"
17          - name: ADD_SERVER_IP_TO_COMMAND
18            value: "true"
19        securityContext:
20          privileged: true
21        resources:
22          requests:
23            memory: "64Mi"
24            cpu: "100m"
25          limits:
26            memory: "128M"
27            cpu: "200m"
28        region: 'ids-rj'
```

Vítima - Ataque nº 2

Parte do código responsável pelo servidor

```
1 Experiment:
2   name: mentored_experiment
3   nodeactors:
4     - name: 'na-server'
5       persitent_volume_path: "/app/packets.pcap"
6       replicas: 1
7       containers:
8         - name: tshark
9           image: ghcr.io/mentoredtestbed/mentored-tshark
10          command: ["/entry.sh"]
11          args: ["tshark", "-i", "net1", "-x", "-w", "packets.pcap"]
12          env:
13            - name: TIMEOUT_CMD
14              value: "300"
15          - name: 'server'
16            image: ghcr.io/mentoredtestbed/generic-apache-flask-webserver:latest
17            env:
18              - name: ENABLE_SLOWLORIS_DEFENSE
19                value: "true"
20            ports:
21              - containerPort: 80
22            resources:
23              requests:
24                memory: 1G
25                cpu: "1"
26              limits:
27                memory: "2G"
28                cpu: "2"
29            region: 'ids-go'
```

```
1   # Check if the variable ENABLE_SLOWLORIS_DEFENSE is true
2   <IfModule mod_reqtimeout.c>
3       RequestReadTimeout header=20-40,MinRate=500 body=20-40,MinRate=500
4   </IfModule>
```

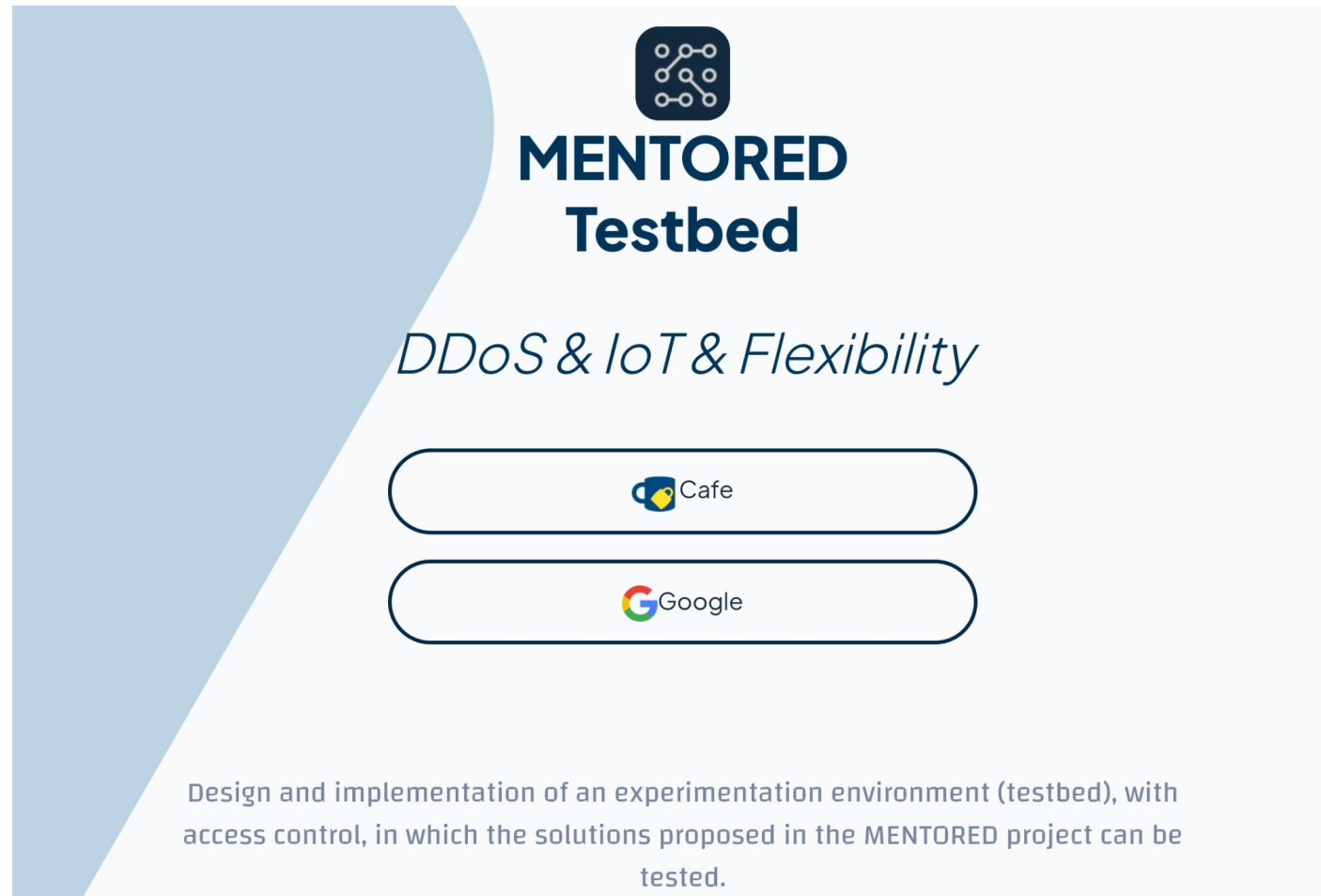
Vítima - Troca de Imagem

Parte do código responsável pelo servidor

```
1 Experiment:
2   name: mentored_experiment
3   nodeactors:
4     - name: 'na-server'
5       persitent_volume_path: "/app/packets.pcap"
6       replicas: 1
7       containers:
8         - name: tshark
9           image: ghcr.io/mentoredtestbed/mentored-tshark
10          command: ["/entry.sh"]
11          args: ["tshark", "-i", "net1", "-x", "-w", "packets.pcap"]
12          env:
13            - name: TIMEOUT_CMD
14              value: "300"
15        - name: 'server'
16          image: ghcr.io/mentoredtestbed/generic-apache-flask-webserver-modqos:latest
17          ports:
18            - containerPort: 80
19          resources:
20            requests:
21              memory: 1G
22              cpu: "1"
23            limits:
24              memory: "2G"
25              cpu: "2"
26          region: 'ids-go'
```

Atividade Prática

Login no portal do MENTORED *Testbed*



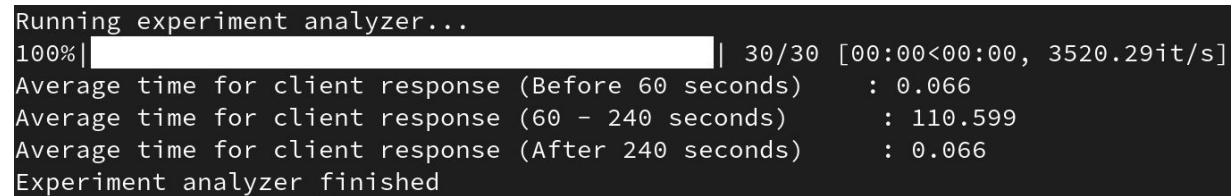
*<https://portal.mentored.ccsc-research.org>

Resultado

Arquivos resultantes do ataque

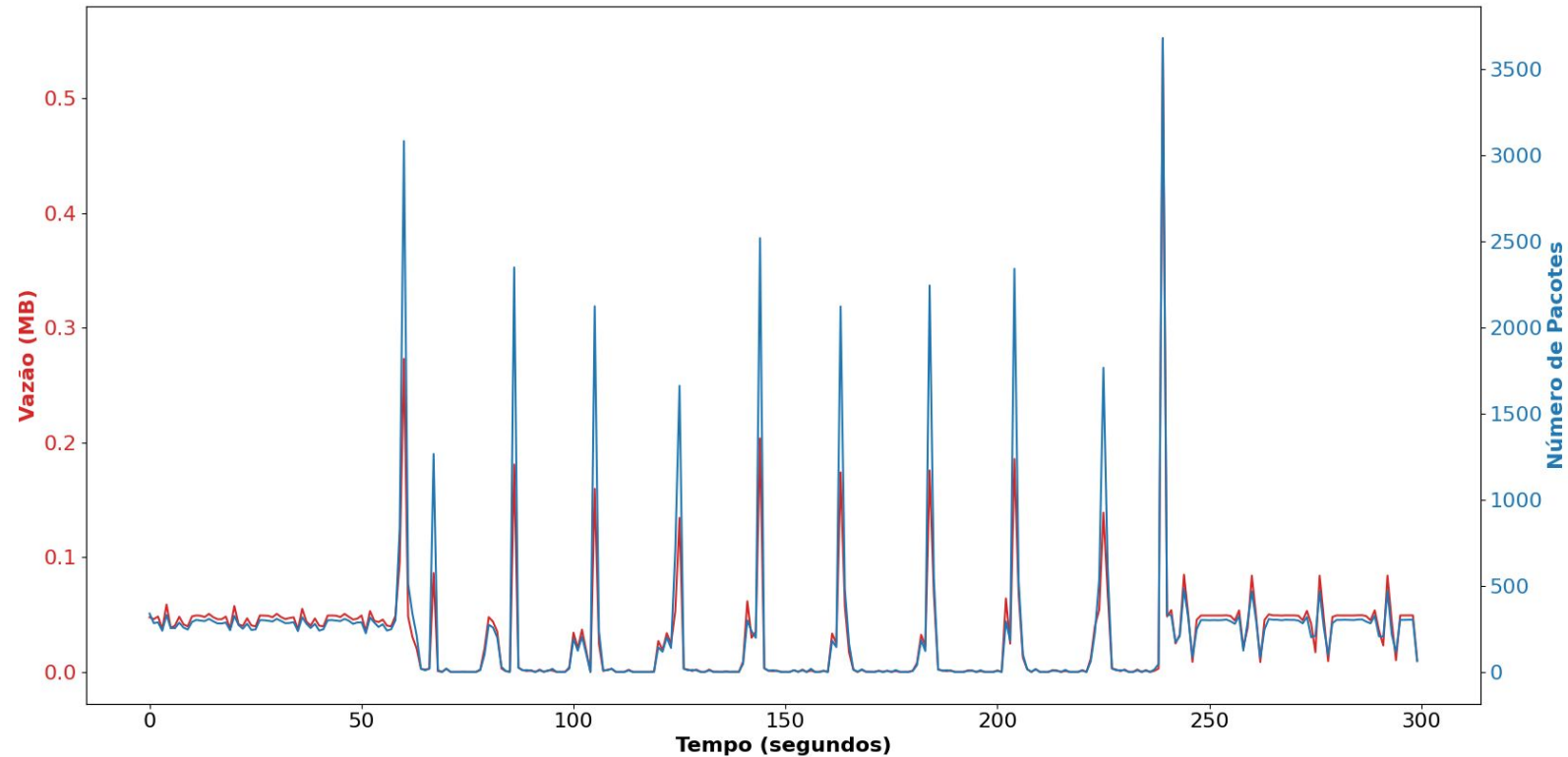
- Arquivo com a captura de tráfego da vítima;
 - *packets.pcap*
- Arquivos com o tempo de respostas das requisições GET dos clientes;
 - *client_delay.csv*
- Arquivo contendo a lista de todos os IPs classificados por tipo e região;
 - *MENTORED_IP_LIST.yaml*
- Arquivo contendo os *logs* do experimento;
 - *experiment_logs.tar*
- Ferramentas utilizadas na criação dos gráficos;
 - <https://github.com/mentoredtestbed/demo-wtestbed-csbc-2024>





Ataque nº 2

Resultado do ataque com Slowloris modificado



Running experiment analyzer...

100% |

Average time for client response (Before 60 seconds) : 0.066

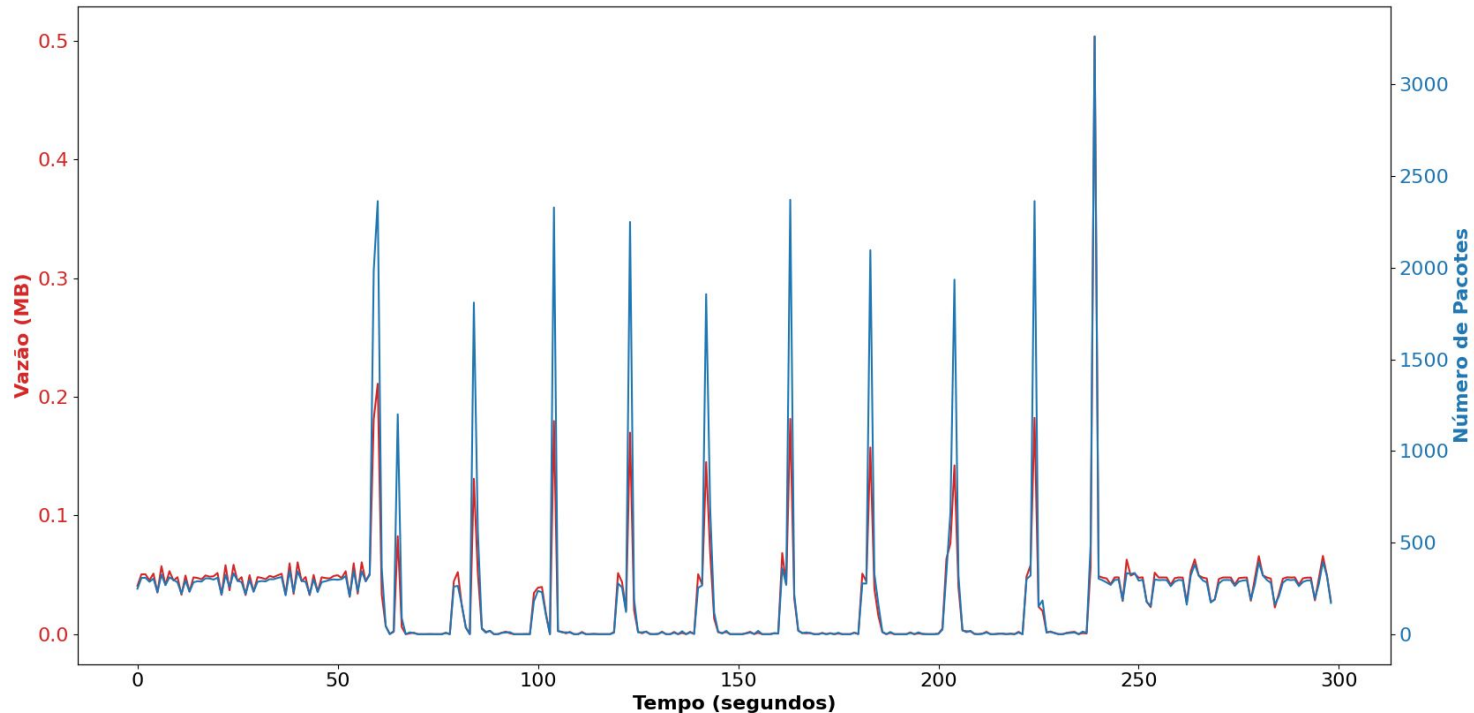
Average time for client response (60 - 240 seconds) : 43.005

Average time for client response (After 240 seconds) : 0.067

Experiment analyzer finished

Exemplo

Resultado do ataque com Slowloris mod_qos



Running experiment analyzer...

100%|

Average time for client response (Before 60 seconds) : 0.066

Average time for client response (60 - 240 seconds) : 41.559

Average time for client response (After 240 seconds) : 0.067

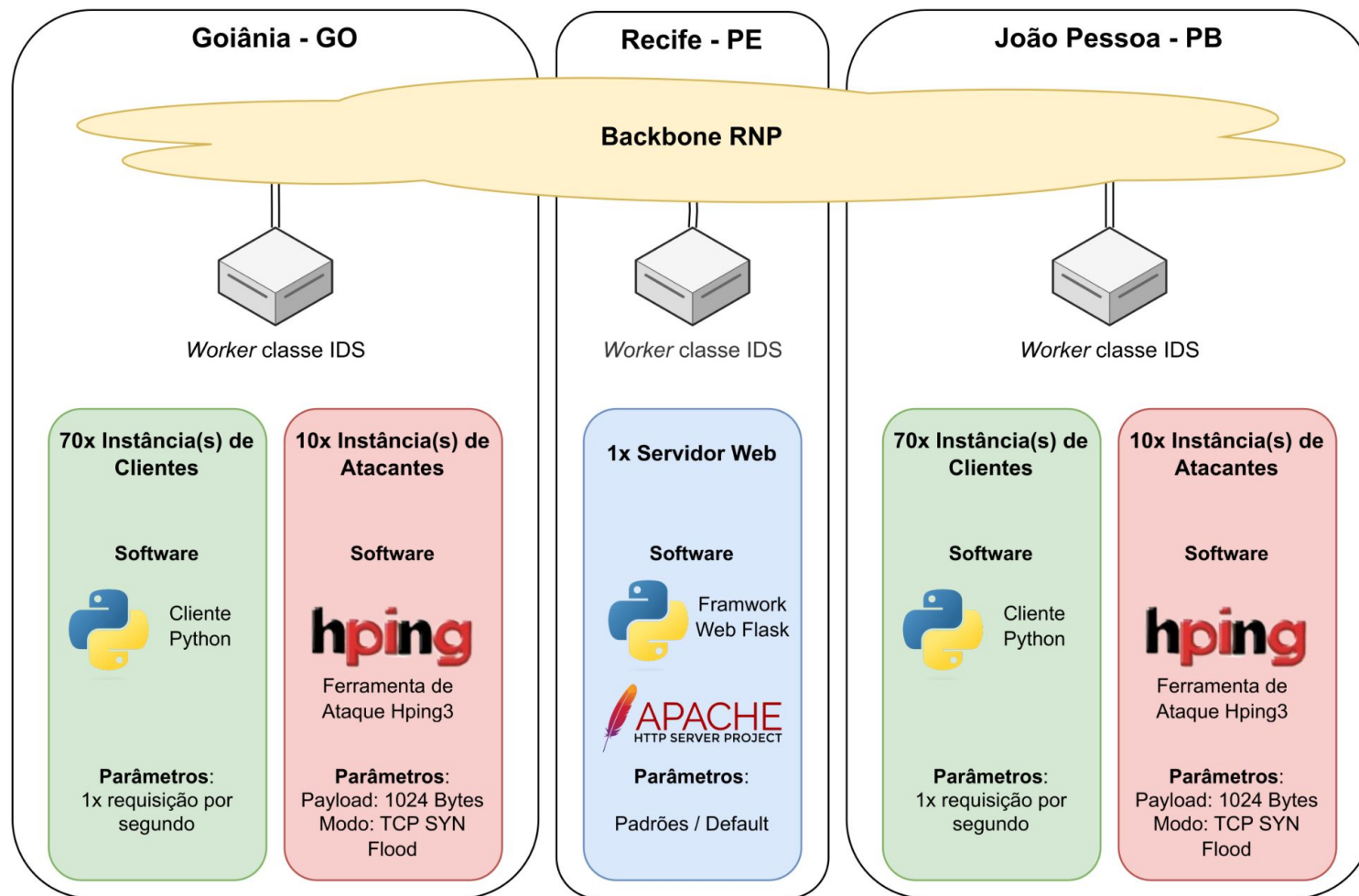
Experiment analyzer finished

Capítulo do Livro

Configuração do ataque com Hping3



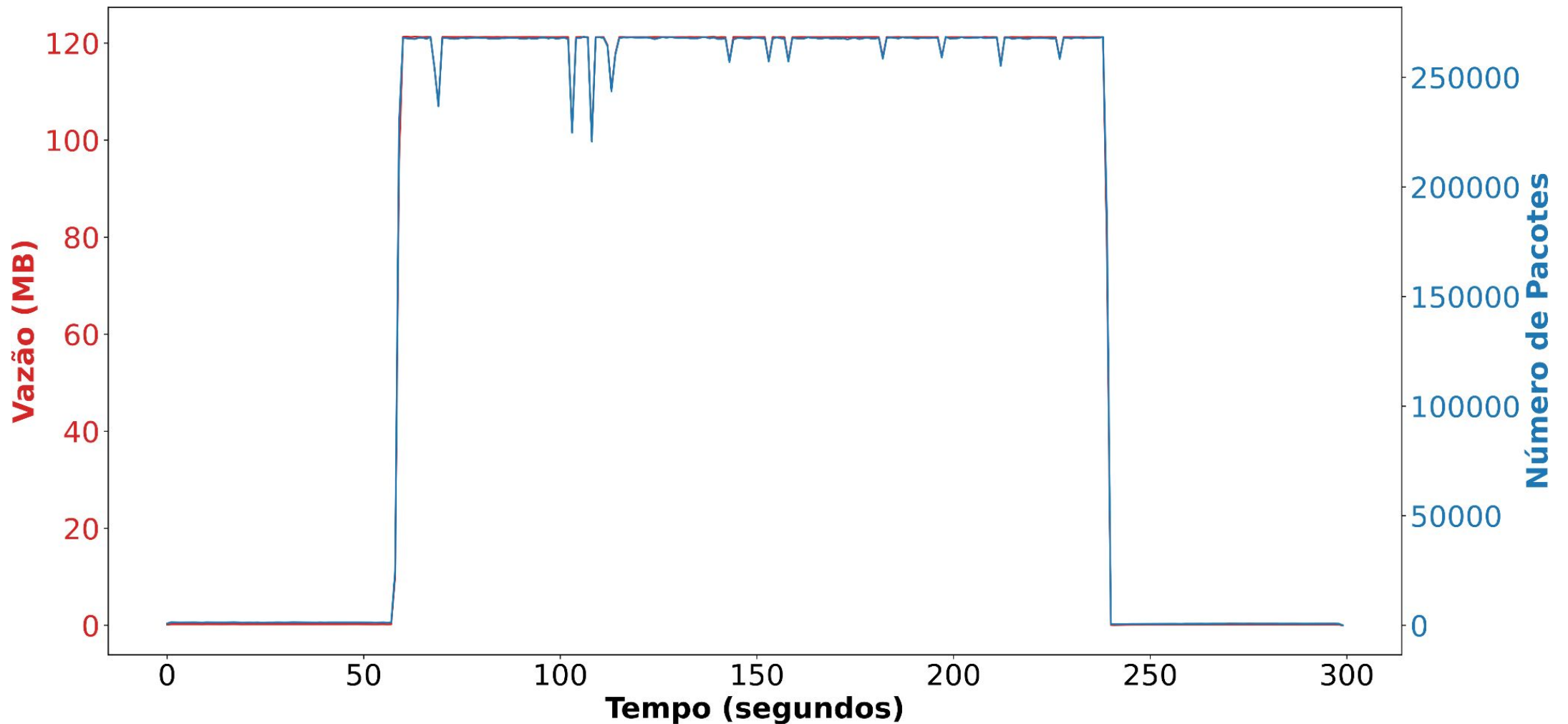
Capítulo
Minicurso SBRC 2024



Repositório GitHub
Minicurso SBRC 2024

Hping3

Gráfico com o ataque utilizando o Hping3



Considerações Finais

Q&A



Site do Projeto
MENTORED



Repositório GitHub
Demo *WTestbed* CSBC 2024

Analizando ataques Slowloris com o **MENTORED** *Testbed*

Apresentadores:

- Michelle S. Wingham | UNIVALI/RNP
- Davi D. Gemmer | RNP

