Cyber Range Scenarios

Use of a solver to generate scenarios for cyber ranges based on contextual information

Benoît Duhoux *(UCLouvain), Axel Legay (UCLouvain), Ramin Sadre (UCLouvain), Suzanne Kieffer (UCLouvain), Justine Ramelot (UCLouvain), Sébastien Dupont (CETIC), Philippe Massonet (CETIC), Maher Badri (CETIC), Guillaume Ginis (CETIC), Matteo Merialdo (RHEA group), Artem Korytnyi (RHEA group), …*

A Win2Wal project

Wallonie recherche SPW

Presented at the researchers' day of CyberExcellence
November 8th, 2022
Mons, Belgium

Cyber ranges (1)

“A cyber range is a virtual training ground for security experts. Trainees are separated into attacking and defending teams, whose roles are either to compromise or to protect some critical infrastructure, composed of various potentially vulnerable assets, including computers, software systems, network topologies and more.” [1]

[1] Pierre Martou, Kim Mens, Benoît Duhoux, and Axel Legay. 2022. Generating Virtual Scenarios for Cyber Ranges from Feature-Based Context-Oriented Models: A Case Study. COP’ 22.

Scenarios

A scenario is composed of a set of hardware components, network topologies, software systems with a specific version that contain vulnerabilities.

Creating scenarios

1. Manually

   Need experts, time-consuming, not really reusable

   But customizable based on user information

2. Automatically

   Costa et al. [2] proposes a Virtual Scenario Description Language (VSDL) to generate scenarios.

   This solution already integrates the use of a solver.

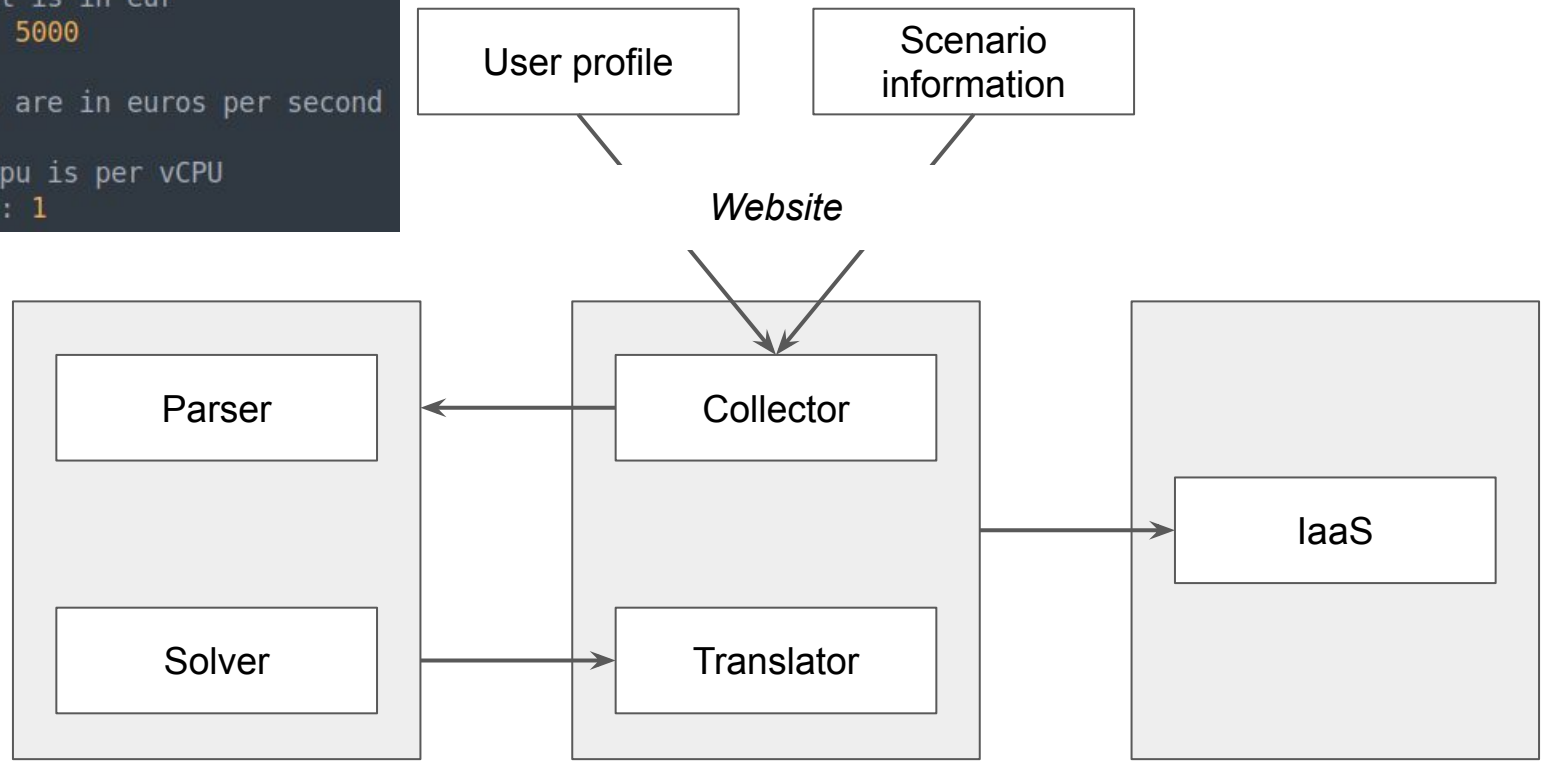
   Less time-consuming but not customizable based on user information

[2] Gabriele Costa, Enrico Russo, and Alessandro Armando. 2020. Automating the Generation of Cyber Range Virtual Scenarios with VSDL. arXiv preprint arXiv:2001.06681 (January 2020).

Our architecture

```
node_types:
  - crs2.be.tosca.nodetypes.rover_w1-wip1:
      requirements:
        - num_cpu:
            occurrences: [ 2, 4 ]
```

```
scenario:
  # duration is in secondes
  duration: 7200
  # budget is in eur
  budget: 5000

  # costs are in euros per second
  costs:
      # cpu is per vCPU
      cpu: 1
```



First prototype (1)

Input

```
scenario:
  # duration is in minutes
  duration: 120
  # budget is in eur
  budget: 5000

  # costs are in euros per second
  costs:
        # cpu is per vCPU
        cpu: 0.1
        # ram is per GB
        ram: 0.1
        # storage is per GB
        storage: 0.01
```

```
  node_types:
        - crs2.be.tosca.nodetypes.rover_w1-wip1:
        requirements:
        - num_cpu:
                occurrences: [ 2, 4 ]
```

Output

```
nodes:
      rover_w1-wip1:
            num_cpu: 3
```

```
nodes:
      rover_w1-wip1:
            num_cpu: 2
```

```
nodes:
      rover_w1-wip1:
            num_cpu: 4
```

First prototype (2)

Input

```
scenario:
  # duration is in minutes
  duration: 120
  # budget is in eur
  budget: 5000

  # costs are in euros per second
  costs:
        # cpu is per vCPU
        cpu: 0.1
        # ram is per GB
        ram: 0.1
        # storage is per GB
        storage: 0.01
```

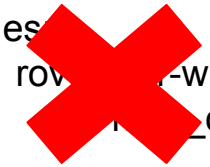
```
  node_types:
        - crs2.be.tosca.nodetypes.rover_w1-wip1:
        requirements:
        - num_cpu:
                occurrences: [ 2, 4 ]
```

Output

```
nodes:
      rover_w1-wip1:
            num_cpu: 3
```

```
nodes:
      rover_w1-wip1:
            num_cpu: 2
```

```
nodes:
      rover_w1-wip1:
            num_cpu: 4
```



First prototype (3)

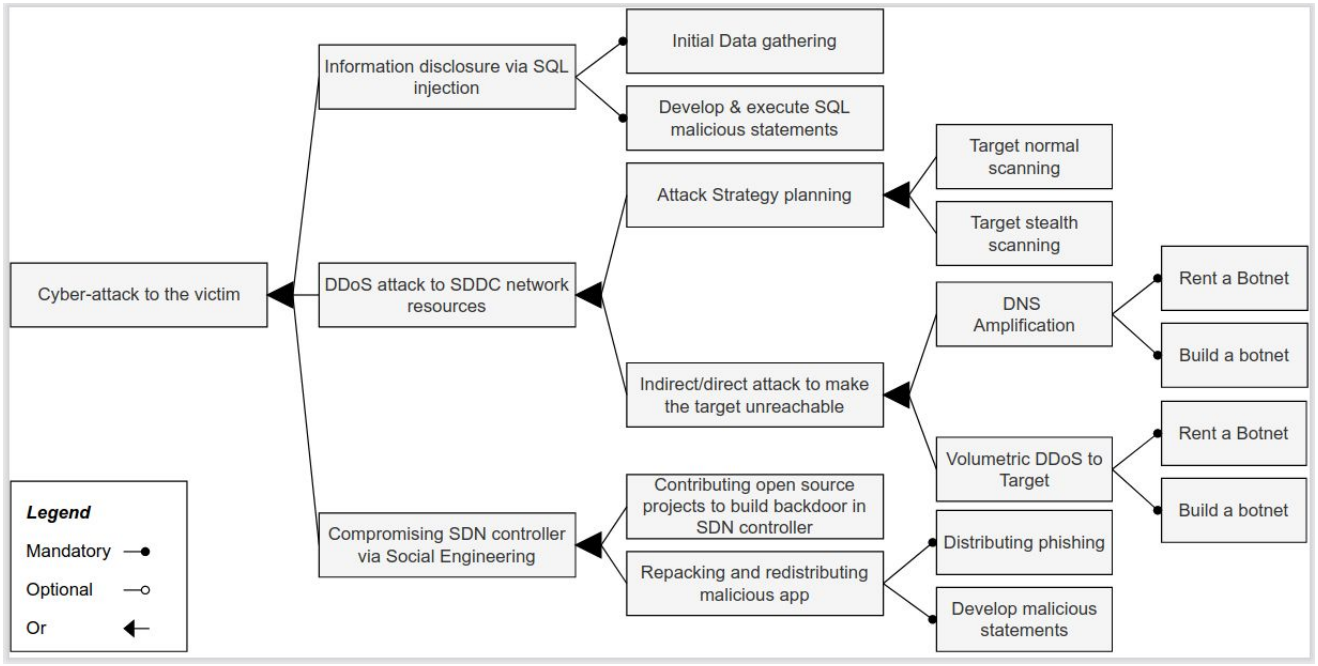
```
scenario:
  # duration is in minutes
  duration: 120
  # budget is in eur
  budget: 5000

  # costs are in euros per second
  costs:
        # cpu is per vCPU
        cpu: 0.1
        # ram is per GB
        ram: 0.1
        # storage is per GB
        storage: 0.01

  node_types:
        - crs2.be.tosca.nodetypes.rover_w1-wip1:
        requirements:
        - num_cpu:
                occurrences: [ 2, 4 ]
```

$$budget \geqslant \sum_{n}^{nodes} \sum_{c}^{cpus} costCpuPerSec * durationPerSec$$

What's next?

Include more variabilities.

Integrate ADTs (Attack-Defense Trees) for a better training assistance.



Pierre Martou, Kim Mens, Benoît Duhoux, and Axel Legay. 2022. Generating Virtual Scenarios for Cyber Ranges from Feature-Based Context-Oriented Models: A Case Study. COP' 22.

Minimize / maximize the scenario configuration depending on the user requirements.