Sharing and replaying attack scenarios with moirai

Guillaume Brogi, Valérie Viet Triem Tong
Akheros, Cnam, CentraleSupelec

A high quality and modern dataset is required to evaluate IDS.

Motivation

Datasets are necessary for evaluating and comparing IDS. But, they are set in stone:

- cannot be changed easily
- force the IDS to use its type of input data

Instead, we need something that:

- can be updated and adapted
- can work with any type of input data

What is moirai?

moirai is a tool to help create, replay and share scenarios used for the evaluation of IDS. It tries to keep things simple.

- Scenarios are defined in one `ini` plaintext file, so they can be shared easily
- VM are configured and launched through `Vagrant`
- The actions are done on the VM through ssh and winrm
- moirai itself is written in python and open source

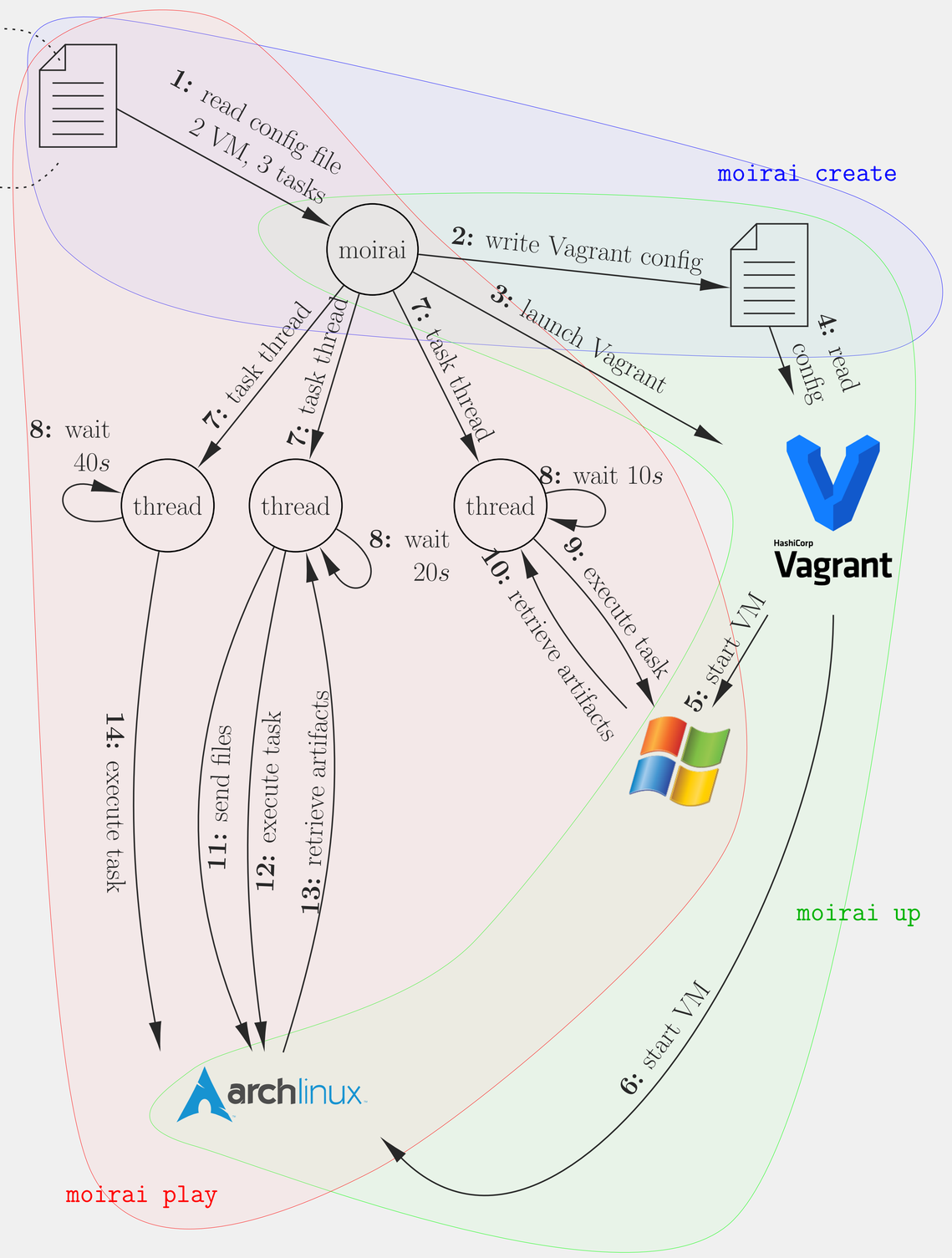
Create scenarios and share them easily!

Let's play with moirai: https://github.com/akheros/moirai

Configuration file

```
[Cluster]
machines = winxp, archlinux

[winxp]
box = IE8.XP.For.Vagrant
guest = windows
username = IEUser
password = Passw0rd!
ip = 192.168.51.5
shares = /tmp -> /host_tmp

[archlinux]
box = terrywang/archlinux
box_url = https://mycustom.url/archlinux.box
shares = /tmp -> /host_tmp

[Scenario]
tasks = check_disks, list_files, sleep
duration = 1m

[check_disks]
target = winxp
timing = 10s
actions = wmic logicaldisk get caption > disks.txt
artifacts = disks.txt

[list_files]
target = archlinux
timing = +10s
actions = ls -lah > file_list
files = .bashrc
        .bash_history -> history
artifacts = file_list -> archlinux_ls

[sleep]
target = archlinux
timing = +20s
actions = sleep 120
          uname -a
```

Enumerate the machines
Base Vagrant box
Custom configuration
List of tasks
Maximum duration
VM to act on
When to act
What to do
Files to send
Artifacts to retrieve
Relative to the previous task



Contact:

Guillaume Brogi `guillaume.brogi@akheros.com`

- **moirai:** `https://github.com/akheros/moirai`
- **public scenarios:** `https://github.com/akheros/moirai-scenarios`

AKHEROS
le cnam
CentraleSupélec