WP4 focuses on testing and demonstrating platform and methods which developed other WPs. It contains following elements:

- Develop a testing environment which could evaluate this project’s outcomes
- Demonstrate and Evaluate case studies

Testing Environment

We agreed to adapt a virtual machine environment for the demos due to the diversity of multiple scenarios on WP4. Therefore, we require flexibly in order to set up demonstration environments for each scenario. Accordingly, we chose the following tools for constructing the environments.

- **virtual machine environment**
  - **KVM**: a hypervisor (HV) for the virtual machine environment.
  - **virtsh**: provides controlling and management functions for KVM. The tool creates, configures and deletes guest VMs on HV machines.

- **automatic deployment**
  - **MAAS**: a software to install OS images on bare metal machines. It can automate the installation process of the OS (Ubuntu).
  - **ANSIBLE**: an automation tool to configure hosts based on predefined settings. The tool is used to set up software on hosts.

Testing Scenarios

1. **DDoS Mitigation - DNS Amplification Attack**

   This scenario supposes a major DDoS attacking method which known as ‘DNS Amplification Attack’. In this scenario, ‘detector’ detects series of attack and reports it through ‘NECOMAter’. ‘mitigator’ orders ‘mitigator switch’ to control these detected attacks.

2. **Botnet Introspection – detecting C&C servers**

   This scenario shows a botnet detecting and investigating mechanism which developed on this project. This system continuously analyzes traffic data to find out C&C servers and Botnet clients in their network. An analyzing method uses two kinds of network traffic – 1) DNS queries from Botnet client sandbox, 2) DNS queries from their commodity network. Using machine learning method which developed in this project, the system maintain a blacklist of C&C server. When botnet clients attempt to connect C&C servers, it will be induced to our ‘Decoy’ C&C server to investigate their traffic.