Honeypot Testbed for Network Defence Strategy Evaluation

Jana Medková, Martin Husák, Martin Vizváry, Pavel Čeleda

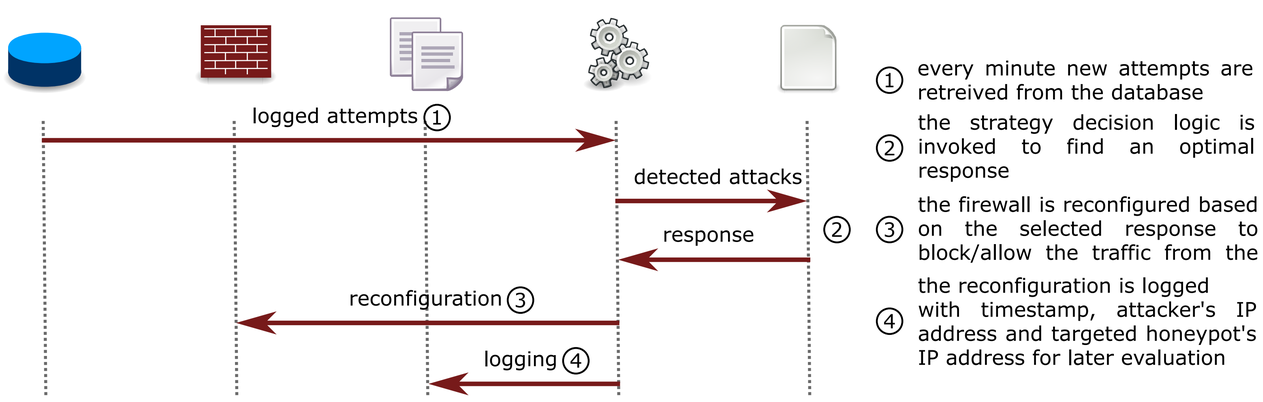
Masaryk University, Institute of Computer Science
Brno, Czech Republic

{medkova, husakm, vizvary, celeda}@ics.muni.cz

Abstract

We present a network defence strategy testbed, which could be utilized for testing the strategy decision logic against simulated attacks or real attackers. The testbed relies on a network of honeypots and the high level of logging and monitoring the honeypots provide. Its main advantage is that only the decision logic implementation is needed in order to test the strategy. The testbed also evaluates the tested network defence strategy. We demonstrate an example of network defence strategy implementation, the test setup, progress, and results. The source code of the testbed is available on GitHub at https://github.com/csirt-mu/DefenceStrategyTestbed.

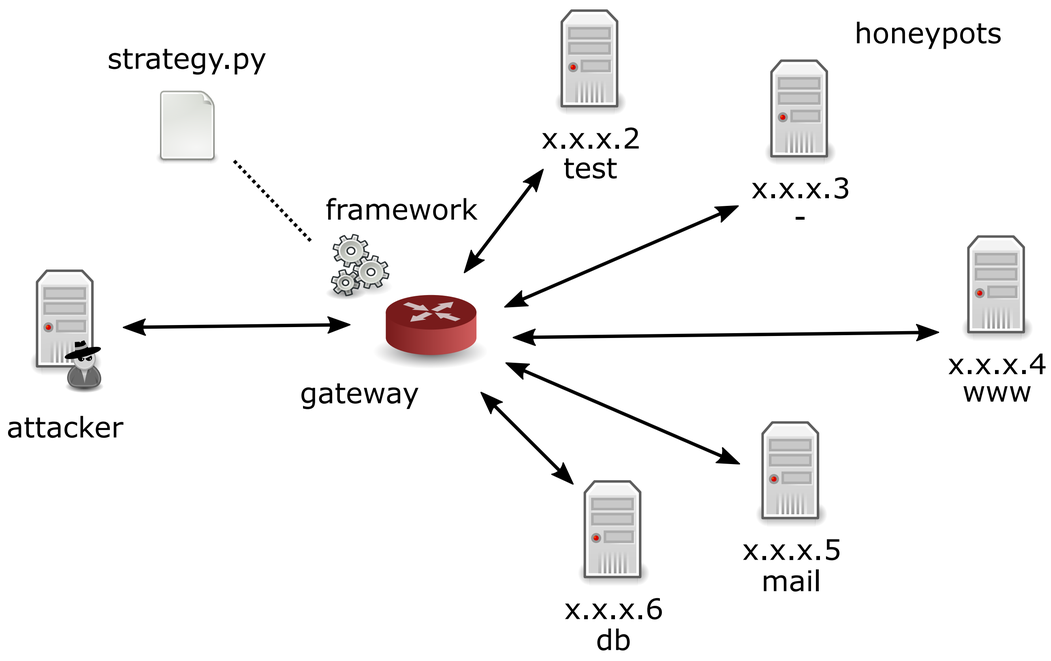
Strategy Execution



Strategy Implementation

```python
#base class with helper methods
class DefenceStrategyBase:
    #provides config values such as
    #damage in case of a successful attack,
    #unavailability cost and reconfiguration cost
    def get_configuration(self):

    #provides current firewall state
    def get_firewall_state(self, srcip):

    #unblocks the target from attacker
    #logs the action into JSON log file
    def unblock(self, srcip, dstip):

    #blocks the target from attacker
    #logs the action into JSON log file
    def block(self, srcip, dstip):

#strategy implementation
class DefenceStrategy(DefenceStrategyBase):
    #takes the list of attacks since the last
    #time the strategy was run and outputs
    #optimal response according to the strategy
    def defend(self, attacks):
```

Testbed Topology



Honeypot

- high-interaction honeypots in a subnet
- SSH server with password authentication that responds to authentication attempts
- logging of authentication attempts into a central database

Gateway

- stores central database of authentication attempts
- executes strategy script
- manipulates firewall rules based on the strategy output

Attacker

- execution of attacks in simulated scenarios

Summary

+ Interaction with real attackers
+ Detection and response capabilities are provided by the framework
+ Strategy input parameters are easy to estimate
+ Excellent monitoring of systems and evaluation
– Basic scenario
– Attacker sooner or later finds out he is interacting with honeypot
– Limited amount of attacks

Acknowledgement

This research was supported by the Security Research Programme of the Czech Republic 2015 - 2020 (BV III / 1 VS) granted by the Ministry of the Interior of the Czech Republic under No. VI20162019014 Simulation, detection, and mitigation of cyber threats endangering critical infrastructure.

The testbed is hosted in Kypo - https://www.kypo.cz

CSIRT-MU