Cloud-based Testbed for Simulation of Cyber Attacks

D. Kouřil, T. Rebok, T. Jirsík, J. Čegan, M. Drašar, M. Vizváry, J. Vykopal

{lastname}@ics.muni.cz

IEEE/IFIP Network Operations and Management Symposium, NOMS 2014
5-9 May 2014, Krakow, Poland
Part I

Introduction
Motivation

Current status

- Ubiquitous cyber attacks
- Need to be studied and understood

What do we need?

- Real-world arrangements simulation
- Sufficient isolation and control
- User friendly environment (easy to instantiate and use)
Requirements statement

- Network-related requirements
- Host-related requirements
- Monitoring infrastructure
- Control requirements
- Deployment requirements
Part II

Cybernetic Proving Ground
About

Features

- Simulation of a large network, systems, services and applications.
- Monitoring of network behaviour, detection and mitigation of anomalies and attacks.
- Cloud environment for repeatable investigation of cyber threats.

Cloud

- Enables computing of resource-intensive tasks.
- Remote secure access of users around the world.
- Enables providing CPG to third parties as a service.
General architecture

Multiple Users

Various Scenarios

Entry Node

Sandbox 1

Sandbox 2

Sandbox n

Scenario Management Node

Cloud environment

Kouřil et al. Cloud-based Testbed for Simulation of Cyber Attacks 7 / 19
Sandbox architecture

- Scenario Management
- Scenario Configuration
- Data Processing
- Database

Network traffic

Management & Measurement channel
ISO Layers

- L2 layer is provided by CPG
- L3 completely under user control

Flexibility

- IPv4, IPv6
- Non-IP protocols
- Emulation of various network characteristics (delays, bandwidth limits, dropped packets)

Components

- Management Network
- Simulated Network
- Lan Management Node
L2 Architecture
L3 Architecture

- DHCP
- Open vSwitch
- Mgmt
- WAN
- firewall
- netem/tc
- Network traffic
- Measured data
- probe
- DHCP

Kouřil et al.  Cloud-based Testbed for Simulation of Cyber Attacks 11 / 19
Monitoring infrastructure

Network monitoring

- Network flow monitoring
- Automatic configuration

Host monitoring

- Nested virtualization
- munin

Probe

Collector

IPFIX

SRC and DST IP addr
SRC and DST port
Protocol number
TCP flags
Lifetime
Sum of bytes
Others

Data analysis

Kouřil et al.
Cloud-based Testbed for Simulation of Cyber Attacks
Benefits for users

Easier investigation of cyber threats and attack

- Automated gathering and processing of data generated during security scenarios.
- Creating database of malicious code (malware, worms, botnets).
- Visualization of significant aspects of the scenarios.

Traffic analysis and forensics

- Acquisition, storage and analysis of network traffic statistics.
- Analysis of malware – at infected host as well as in network.
- Validation of processes of incident handling and response.
Part III

Use-cases
Security scenario

What is it?

- General description of environment, components, actions, expected outcomes of particular experiment

What does it consist of?

- Scenario description
- Technical description
  - Variation description
  - Network topology including node types
  - List of events
  - List of actions
  - Characteristic manifestations
Simulation of DDoS
Attacks to critical infrastructure: Domain Name System

- Testing tools
- Research and development

Forensic analysis of infected files and applications

- Observation and monitoring of captured artifacts
- Scenario repeatability

Penetration testing

- Testing of detection tools
- Training of penetration testers
Future work

Training of security teams
- Commented analysis of scenarios
- Cyber war game in CPG

CPG as a service
- Remote access to CPG to third parties
- New scenarios “on demand“
Thank You For Your Attention!

Cloud-based Testbed for Simulation of Cyber Attacks

D. Kouřil
T. Rebok
T. Jirsík
J. Čegan
M. Drašar
M. Vizváry
J. Vykopal

Home page
http://www.muni.cz/ics/kypo