Cloud Infrastructure Telco Taskforce

Virtual LFN Developer & Testing Forum – June, 2020

RA-1
Security and Testing for security

Karine Sevilla
June 25, 2020
Agenda

› Status on RA-1 security
  ‣ what we have
  ‣ what we need to expand

Common security requirements with ONAP

› Security Testing
  ‣ How to validate RA-1 security requirements?
    ‣ Tests available
    ‣ Testing tools
    ‣ Gaps

› Action Plan
Status on RA-1 Security

› RA-1 security requirements = RM security requirements applied to infrastructure based on OpenStack

› Security requirements in RA-1 Chapter 2
https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter02.md#2.3.8

› Security Content in RA-1 Chapter 6
https://github.com/cntt-n/CNTT/blob/master/doc/ref_arch/openstack/chapters/chapter06.md

› RA-1 security coverage
  › Platform access
  › System Hardening
  › Confidentiality and Integrity
  › Workload security
  › Image security
  › Security LCM
  › Security Audit logging

› Application/VNF workload security: out of scope
RA-1 Security: Evolution for Baraque release

 › Expand RA-1 Security Chapter to address all the security requirements coming from RM
   › We need more contributors to provide content on topics such as
     › System hardening
     › Image security
     › Monitoring and audit

 › Review RM requirements
   › Some requirements too generic must be clarified
     sec.wl.002: The Platform **must** support operational security
     sec.wl.005: Production workloads **must** be separated from non-production workloads
     sec.gen.012: The Operator **must** ensure that only authorized actors have physical access to the underlying infrastructure.
     sec.wl.006: Workloads **must** be separable by their categorisation (for example, payment card information, healthcare, etc.)
Common security requirements with ONAP

- Analysis on going on ONAP security requirements
  
  https://wiki.lfnetworking.org/display/LN/RM+and+RA1%3A+ONAP+Security+Requirements

- Take advantage of this effort to improve RA-1 with missing requirements
Testing for security RA-1 -> RC-1

- Testing
  - Mandatory security requirements to be validated via automated testing as much as possible
  - 4 categories of requirements
    - Requirements automatically fulfilled by design using OpenStack
    - Requirements validated via automated testing
    - Requirements validated via manual testing
    - Requirements validated using specific security tools
  - Refine the CNTT scope on security testing regarding requirements not part of these categories
Security Tests

› What are the security tests relevant and already available?
  › VM images scan, Docker images scan
  › Configuration files and binaries integrity check
  › Verification of QEMU/KVM hardening via checksec.sh
  › OpenStack security Checklist (Security Guide) for Keystone, Horizon, Nova, Cinder, Neutron
  › OpenStack Patrole for RBAC testing
  › CIS (Center for Internet Security) benchmarks
  › …
Security tools

› What are the existing testing tools?
  › CIS-CAT (Configuration Assessment Tools)
  › OpenSCAP (Open Security Content Automation Protocol)
  › AIDE (Advanced Intrusion Detection Environment)
  › …
Action Plan

› Objective for Baraque release
   › Complete RA-1 Security chapter with missing security items
   › Identify the relevant security tests available
   › Identify the relevant security tools available
   › Integrate as much as possible the tests into Xtesting framework to automate the testing
› Other ideas?
Thanks!