Investigating Cloud Virtual Network Isolation Security

Haifa Al Nasseri: hmkan@st-andrews.ac.uk
Dr. Ishbel Duncan: Ishbel.Duncan@st-andrews.ac.uk

May 2017

University of St Andrews

Sultanate of Oman
Ministry of Manpower

Abstract

- **Software Defined Networking (SDN)** or **Virtual Networks (VNs)** are required for cloud tenants to leverage demands.
- **Multi-tenancy** can be compromised without proper isolation.
- Much research has been conducted in **VN Isolation (VNI)**; however security aspects are not tackled.
- **Data leakage** is a major security concern in the cloud.
- This research uses **OpenStack Tenants VNs** to **test multi-tenancy features**.
- Through using penetration tests, **this research aims** to:
  1. **Identify vulnerabilities** causing cloud VN data leakage.
  2. **Investigate** how vulnerabilities and leaked data can **compromise** the tenant Virtual Networks,
  3. **Determine** how **best practices** can be used to reduce the data leakage of the Cloud Tenant VNs caused by improper implementation of isolation mechanisms.

Problem Statement

Cloud Virtual Networks (CVN) are a prime source of information and Cloud Providers must ensure security through isolation. However, some isolation mechanisms are not secure and the information held within is not private.

Hypothesis 1 (H1): OpenStack Cloud Tenant1 can use pentesting to discover VN Isolation information about OpenStack Cloud Tenant2 using ***an external attack*** (Kali outside Cloud).

Hypothesis 2 (H2): OpenStack Cloud Tenant1 can use pentesting to discover VN Isolation information about OpenStack Cloud Tenant2 using ***an internal attack*** (Kali as a Cloud VM in Tenant1).

Objectives:

- Build test Cloud to analyse CVNI using OpenStack. (**Test Bed**)
- Find VNI mechanisms used by the cloud. (**Experiment 1**)
- Check leakage at nodes, bridges, namespace, etc. (**Experiment 2 (H1) & Experiment 3 (H2)**)
- Suggest best practices to reduce/eliminate VN leakages.

Methodology

Testbed: Built Multi-Node OpenStack/Mitaka Cloud under virtualized environment on Gorman Server (Figure 1).
Tenants, users, VMs and VNs were created as examples of cloud tenant components shown in Figure 2 & 3.

Deep Dive: OpenStack Network infrastructure deep dive; using white box testing with administrator privileged scripts to test tenant VN components. Outputs were collected, analysed and translated into diagrams to highlight the VN isolation mechanisms used, such as VLAN, GRE, namespaces (qdhcp, qrouter) (Figure 2 & 3).

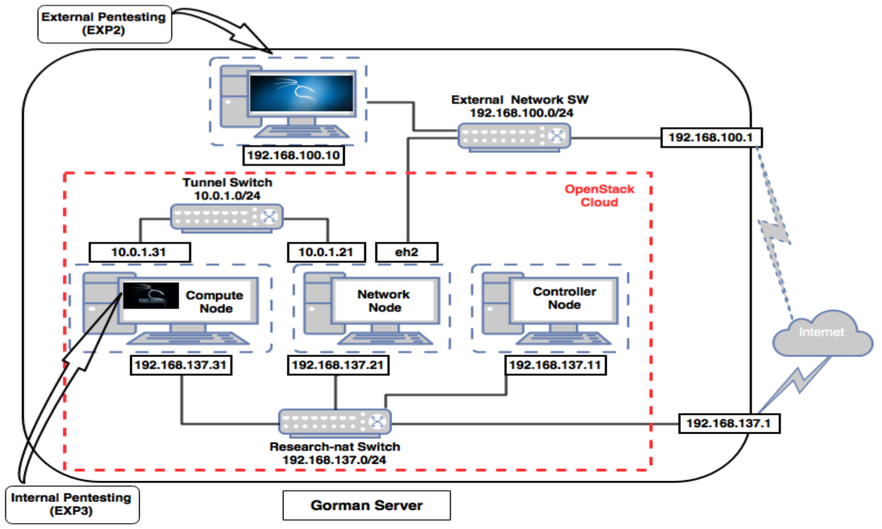

Figure 1: Multi-Node OpenStack Cloud with External (H1- Exp2) and Internal (H2- Exp3) Penetration Test

External (H1) & Internal (H2) Pentesting: Testing Hypothesis 1 & 2; penetration testing was used to find any tenant VN information that is considered an isolation violation and data leakage occurrence (Figure 1).

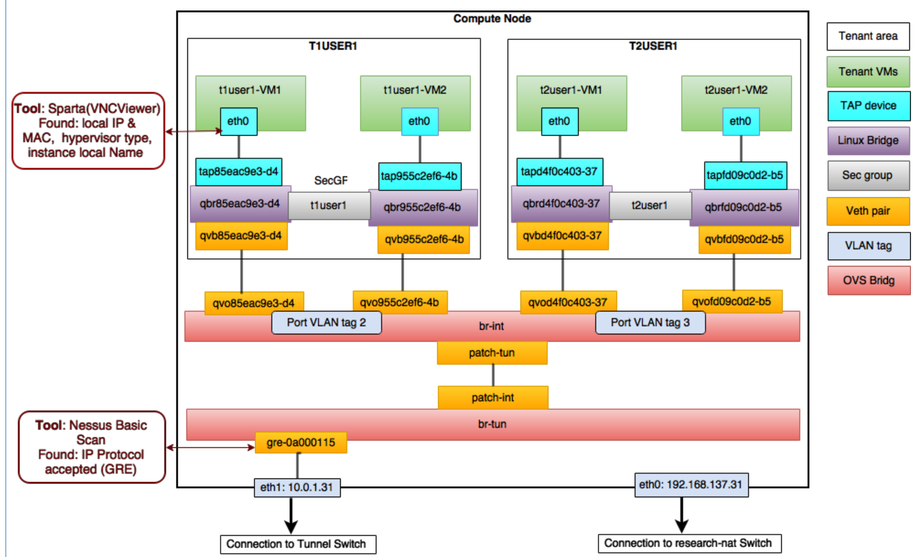

Figure 2: : Cloud Network Infrastructure Deep Diving Part 1 (EXP1) with Pentesting Tools' Results Found in Compute Node

Results

Three penetration test tools (**Zenmap, Sparta, Nessus**) caused information leakage of tenant VNs from the OpenStack Network Infrastructure (Figure 2&3)

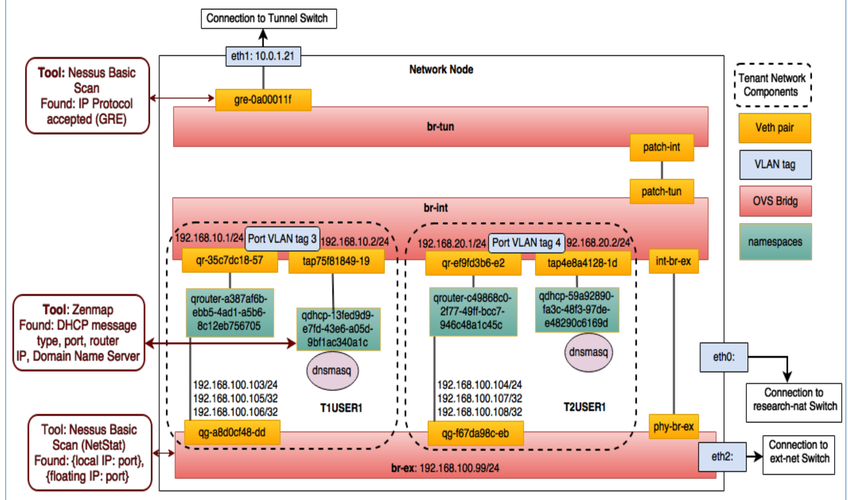

Figure 3: Cloud Network Infrastructure Deep Diving Part 2 (EXP1) with Pentesting Tools' Results Found in Network Node

Conclusions & Future Work

- An **investigation of VN isolation mechanisms** used in an OpenStack cloud to exploit security vulnerabilities through network data leakage has been outlined.
- **OpenStack** has been used as a **testbed** to investigate a virtual network created and managed by the Neutron module.
- An OpenStack Network infrastructure **deep diving method** has been used to reveal the internal cloud network structure and expose the isolation mechanisms OpenStack network infrastructure relies on.
- Several **pentesting stages** (information gathering, scanning, enumeration) have been applied on the testbed and some tenant VN valuable information is leaked by the tools used.
- **Next step:** find vulnerabilities that allow the pentesting tools to cause data leakages and find the best remedy/best practices to reduce/eliminate data leakage occurrences.

References

R. Baloch, Ethical Hacking and Penetration Testing Guide. CRC Press, 2014.
S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," 2015.
Joseph, Elizabeth K., and Matt Fischer. Common OpenStack Deployments: Real World Examples for Systems Administrators and Engineers. Prentice Hall, 2016.
Offensive Security, "Kali Linux Tools Listing | Penetration Testing Tools." [Online]. Available: http://tools.kali.org/tools-listing.
D. Schlosser and M. Jarschel, "Network virtualization: Isolation problems and scalability issues."
H. Moraes, R. V. Nunes, and D. Guedes, "Dcportalsng: Efficient isolation of tenant networks in virtualized datacenters," Proc. 13th ICN, 2014.