POTASSIUM: Penetration Testing as a Service

Richard Li, Dallin Abendroth, Xing Lin, Yuankai Guo,
Hyun-wook Baek, Eric Eide, Robert Ricci, and Jacobus Van der Merwe

THE UNIVERSITY OF UTAH

Current Pentesting

- Impacts production systems
- Interferes with other tenants
- Human intensive
- Restricted in practice (e.g., AWS requires pre-approval)

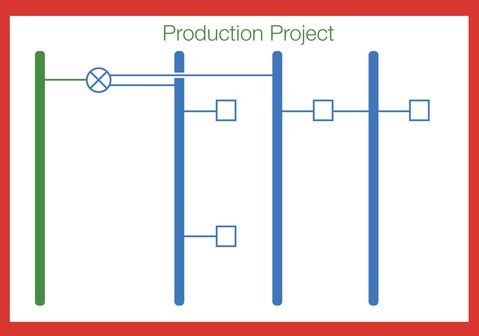
Our Solution

- Make a "clone" of cloud resources
- Isolate cloned resources
- Automate process
- Allow cloud provider to provide penetration testing as a service

Benefits

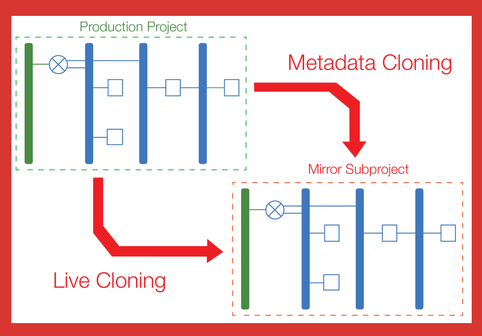
- Availability & scalability
- Safety
- Validity & extensibility
- No harm to production systems or other tenants

How It Works



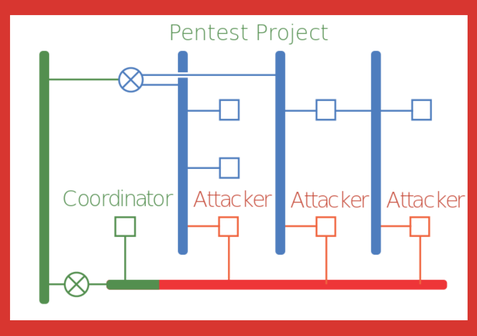
Production Project

- The production project of the cloud tenant.
- Contains VMs and various network objects.



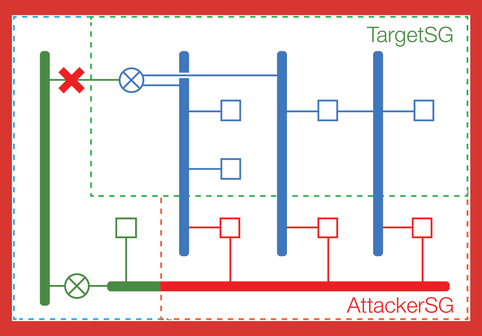
Clone the Project

- Create a new project with the same configuration as the production project.
- Migrate the live state from the production project.



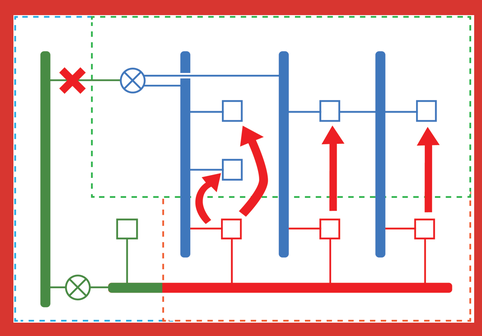
Attacker Creation

- Create attackers in the pentest project.
- Three attack modes: external, internal, pivot.



Security Isolation

- Apply special security groups to attackers and targets.
- Cut off the connectivity to the external network.

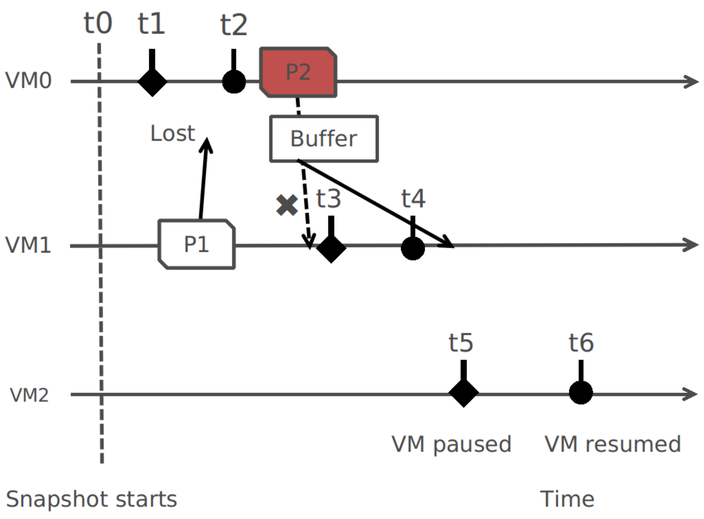


Penetration Testing

- Assign targets to every attacker and do pentesting with Metaspolit.
- Generate the testing report.

Consistent Cloning

Take the snapshot transparently, capturing a globally synchronized state of all VMs in the project [1][2].



Attack Modes

Internal mode: enable attackers to reach every VM in the mirror subproject.

External mode: emulate external attackers from the Internet.

Pivot mode: imitate the way an intruder is able to attack new targets from the point of view of an already compromised VM.

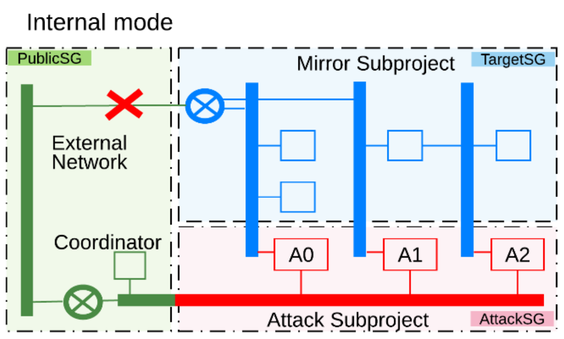
[1] "VNsnap: Taking snapshots of virtual networked environments with minimal downtime," Ardalan Kangarlou, Patrick Eugster, and Dongyan Xu, DSN '09
[2] "HotSnap: A Hot Distributed Snapshot System For Virtual Machine Cluster," Lei Cui, Bo Li, Yangyang Zhang, and Jianxin Li, LISA '13

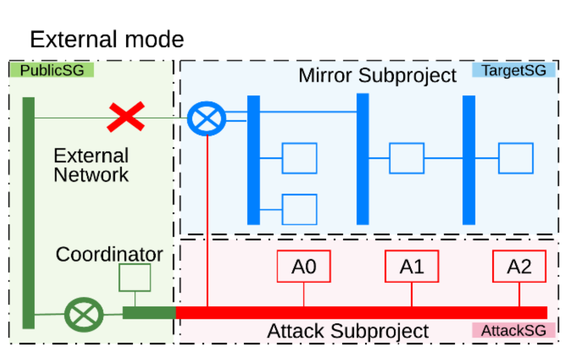
Isolated Pentesting

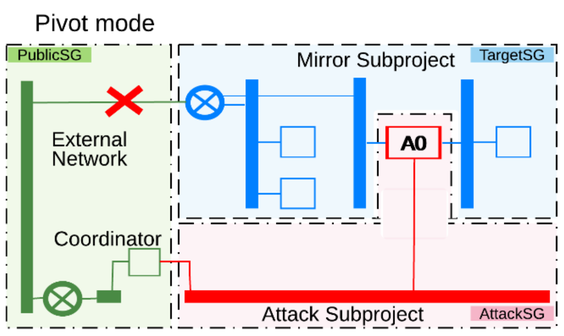
Use availability zone to enforce performance isolation.

Disable network connectivity between mirror subprojects and the external network.

Use security group to ensure attacking traffic only flows between attack and mirror subprojects.







Automated Pentesting

Prototype automated pentester based on Metasploit.

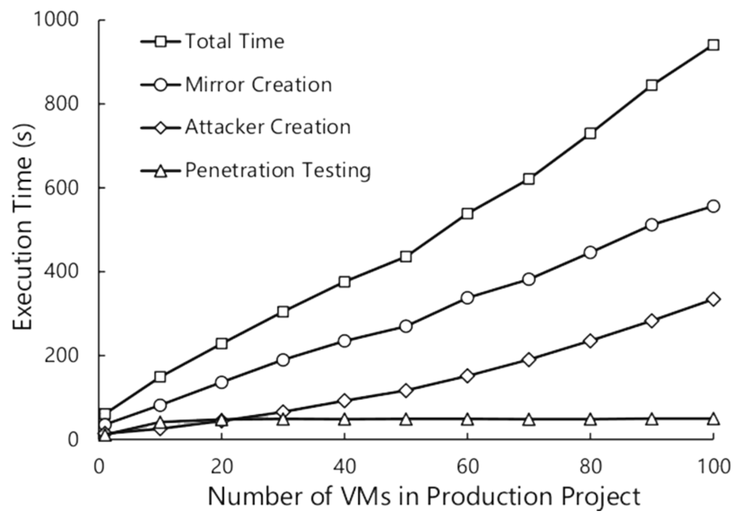
Coordinator instructs attackers to attack by providing the IP addresses of target VMs.

Attackers return attack results to coordinator; pentest manager produces a report.

Scalability Evaluation

We pentest projects containing up to 100 VMs with each attacker targeting 5 nodes.

The total time grows linearly with the size of the production project. The time attackers consume almost stays constant.



This material is based upon work supported by the National Science Foundation under Grant Number 1314945.
Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.