An Ethical Hacking Framework for Assessing Security of Cloud Infrastructure

Phuong Cao, Zbigniew Kalbarczyk, Ravishankar Iyer
University of Illinois at Urbana-Champaign

Harigovind V Ramasamy
IBM Watson Health

Ashish Kundu
IBM T.J. Watson Research Center

Motivation

Although *n-day* vulnerabilities are widely published, existing services are at risk because:

- Services rely on a large number of potentially outdated and vulnerable libraries
- Patching a library in production requires careful planning as it affects other services

Many cloud services still carry known vulnerabilities, e.g., Equifax was affected by a 2-month old vulnerability (CVE-2017-5638).

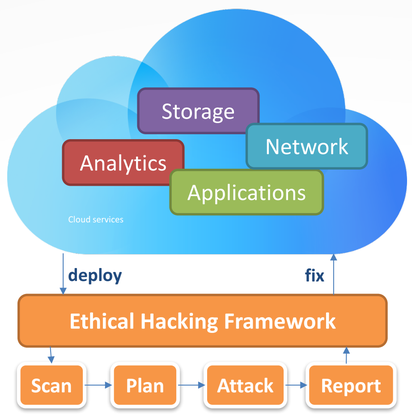


Figure 1. Overview of Ethical Hacking Framework

Problem Definition

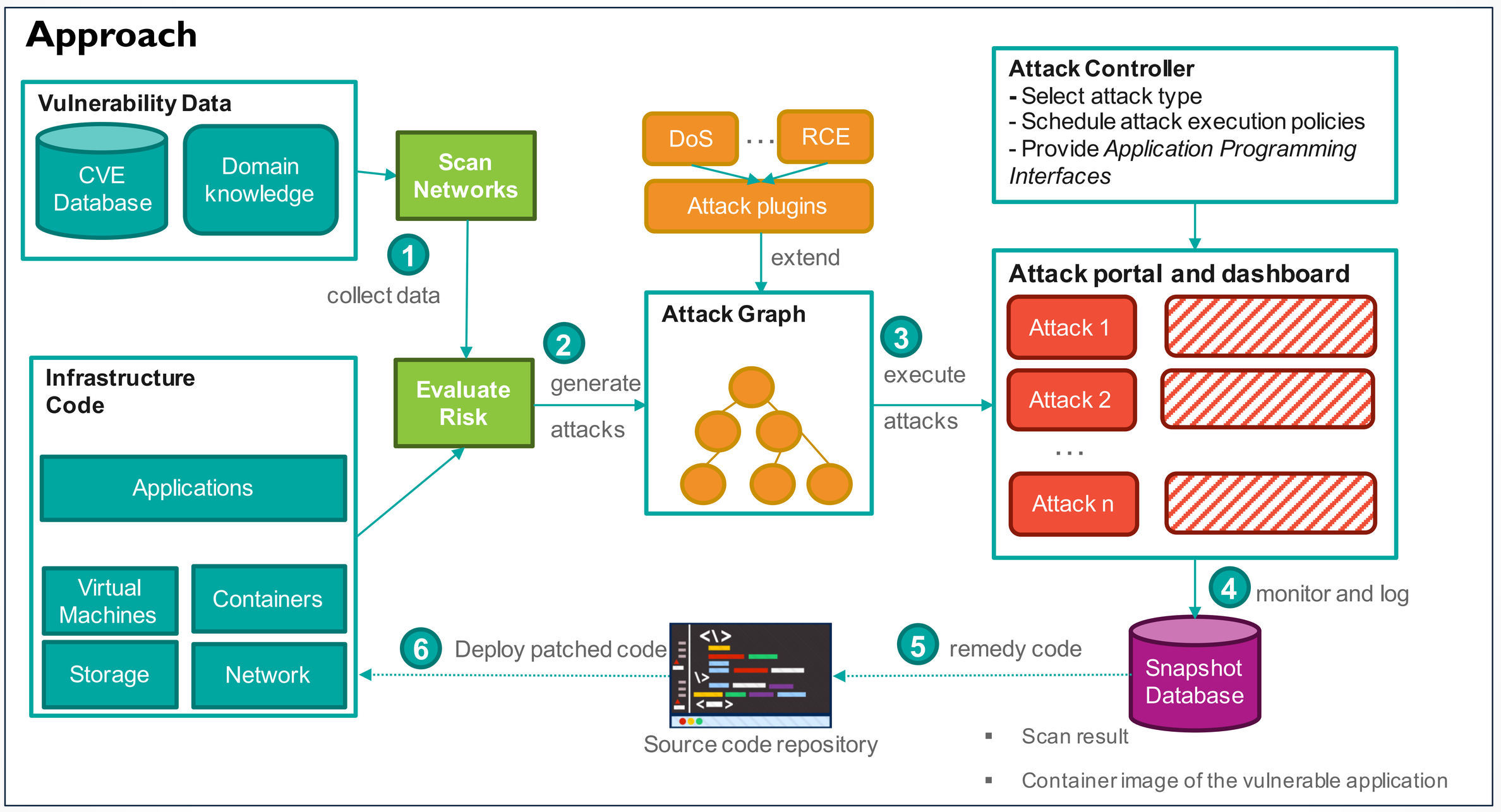
Input. A set of configuration file describing software and network architecture of a cloud service,

Output. Interactive dashboard and security reports

- Existing n-day vulnerabilities in service components,
- Risk evaluation of data, network, and compute modules
- Continuous security testing for a service

The problem is timely as traditional computing, e.g., healthcare analytics, are moving to cloud and critical patient data, e.g., medical records, are at the stake.

Approach



DevSecOps monitoring dashboard

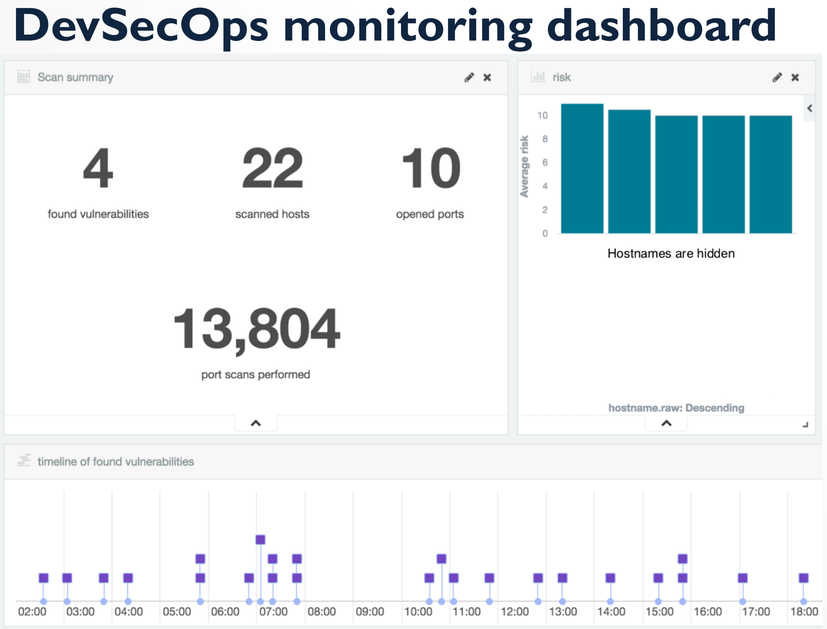


Figure 2. A dashboard showing a timeline of scanned ports, found vulnerabilities, and affected hosts.

Implementation

Attack Type	Status
Information Disclosure	Yes
Slow Denial of Service (targeting Layer-7 applications)	Yes
Volumetric Denial of Service (targeting Layer-3 protocols)	Yes
Autoscaling abuse	Progress
Improper session management	Progress
XSS / SQL Injection	No

Table 1. Classes of attacks targeting cloud services considered in our framework.

Evaluation

Evaluated during one week in August 2016, our framework performed more than 13,000 port scans on 22 hosts in a cloud services development environment.
We highlighted 4 potential vulnerabilities that can be exploited for launching volumetric and slow DDoS attacks.

Conclusion and Future Work

Our remediation step is still manual and requires careful human review of corresponding configuration changes.
We have provided a fast and timely feedback loop for a cloud services development team to fix vulnerabilities.

References

[1] Kula, Raula Gaikovina, et al. "Do developers update their library dependencies?." Empirical Software Engineering, 2017
[2] Lauinger, Tobias, et al. "Thou Shalt Not Depend on Me: Analysing the Use of Outdated JavaScript Libraries on the Web." NDSS, 2017
[3] K. A. Beaty et al., "Managing sensitive applications in the public cloud," in IBM Journal of Research and Development, 2016
[4] Y. Katsuno et al., "Security, Compliance, and Agile Deployment of Personal Identifiable Information Solutions on a Public Cloud," IEEE CLOUD, 2016
[5] Toward a high availability cloud: Techniques and challenges, C Pham et al., DSN-W, 2012
[6] Cooper, Brian F., et al. "Benchmarking cloud serving systems with YCSB." ACM Cloud, 2010.
[7] Disaster Recovery for Cloud-Hosted Enterprise Applications, L Wang et al., IEEE CLOUD, 2016
[8] Hoff, Todd. "Netflix: Continually test by failing servers with Chaos Monkey.", Netflix Blog post, 2010

Acknowledgement

Emma Liddell,, IBM Watson Health,
Yaoping Ruan, IBM Watson Health
Paula Austel, IBM Watson Health Cloud
Diane Frame, IBM Watson Health