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- Services rely on a large number of potentially outdated and vulnerable libraries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).

Problem Definition

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

Output. Interactive dashboard and security reports

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

1. Collect data
2. Generate attacks
3. Execute attacks
4. Monitor and log
5. Remedy code
6. Deploy patched code

References


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

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Disclosure</td>
<td>Yes</td>
</tr>
<tr>
<td>Slow Denial of Service (targeting Layer-7 applications)</td>
<td>Yes</td>
</tr>
<tr>
<td>Volumetric Denial of Service (targeting Layer-3 protocols)</td>
<td>Yes</td>
</tr>
<tr>
<td>Autoscaling abuse</td>
<td>Progress</td>
</tr>
<tr>
<td>Improper session management</td>
<td>Progress</td>
</tr>
<tr>
<td>XSS / SQL Injection</td>
<td>No</td>
</tr>
</tbody>
</table>

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.

Acknowledgement

Emma Liiddell, IBM Watson Health, Yoping Ruan, IBM Watson Health, Paula Austel, IBM Watson Health Cloud, Diane Frame, IBM Watson Health

Figure 1. Overview of Ethical Hacking Framework

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