Automating Vulnerability Assessments with Vuls

Kota KANBE & Teppei FUKUDA
Vuls

- open-source, agent-less vulnerability scanner (based on information from NVD, OVAL, etc.)
Vuls Features In-Depth
Automating Vulnerability Assessments with Vuls | Open Source Summit North America 2017
## Supported OS

<table>
<thead>
<tr>
<th>OS</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubuntu</td>
<td>12, 14, 16</td>
</tr>
<tr>
<td>Debian</td>
<td>7, 8, 9</td>
</tr>
<tr>
<td>RHEL</td>
<td>5, 6, 7</td>
</tr>
<tr>
<td>Oracle Linux</td>
<td>5, 6, 7</td>
</tr>
<tr>
<td>CentOS</td>
<td>6, 7</td>
</tr>
<tr>
<td>Amazon Linux</td>
<td>All</td>
</tr>
<tr>
<td>FreeBSD</td>
<td>10, 11</td>
</tr>
<tr>
<td>Raspbian</td>
<td>Jessie, Stretch</td>
</tr>
</tbody>
</table>
AUTOMATING VULNERABILITY SCANNING WITH VULS

FREEBSD DESKTOP WITH XFCE, SLIM AND I3LOCK

YOUR INFORMATION IS OUT THERE READY FOR BUYING

PROCESSING DATA IN PARALLEL USING MULTITHREADING

THE TRUENAS UNIFIED STORAGE X10

INTERVIEW WITH DAVID MYTTON
Administrator
Agent-less
Automating Vulnerability Assessments with Vuls | Open Source Summit North America 2017

Remote Scan (Agent-less)
Local Scan (Agent mode)
DEMO
Let’s see just how easy it is to use Vuls
Config(TOML)

- Minimum Setting

[servers.centos6]
host = "192.168.33.10"
port = "22"
user = "vuls"
keyPath = "/Users/teppei/.ssh/id_rsa"
Check the Scan Results

- View results with
  - VulsRepo (OSS)
  - TUI (Text-based User Interface)
- Get notifications of results by
  - E-mail
  - Slack
### Heatmap

<table>
<thead>
<tr>
<th>Container</th>
<th>Packages</th>
<th>CVSS Score</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CVSS Severity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.1</td>
</tr>
<tr>
<td>bash</td>
<td>CVE-2016-0634</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-7543</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-6401</td>
<td></td>
</tr>
<tr>
<td>bind-libs</td>
<td>CVE-2016-5804</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-5145</td>
<td></td>
</tr>
<tr>
<td>bind-utils</td>
<td>CVE-2016-5804</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-5145</td>
<td></td>
</tr>
<tr>
<td>coreutils</td>
<td>CVE-2017-2816</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2017-2816</td>
<td></td>
</tr>
<tr>
<td>curl</td>
<td>CVE-2017-2823</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-0718</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-0779</td>
<td></td>
</tr>
<tr>
<td>glibc</td>
<td>CVE-2015-8779</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2017-2825</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-6313</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-1990</td>
<td></td>
</tr>
<tr>
<td>python</td>
<td>CVE-2016-0772</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-0695</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-1000110</td>
<td></td>
</tr>
<tr>
<td>python-libs</td>
<td>CVE-2016-0772</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-0695</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-1000110</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CVE-2016-1248</td>
<td></td>
</tr>
</tbody>
</table>

Automating Vulnerability Assessments with Vuls | Open Source Summit North America 2017
Scanning Modes

Remote (Agent-less)

Vuls Scan Server → Target Server

ssh

Target Container

docker exec

Local (Agent)

Vuls Scan Server → Target Server

Scan

Vuls Scan Server = Target Server

Vuls Scan Server = Target Server
Penetration Testing?  

Non-Intrusive Scans

Pre-authorization not needed when scanning on cloud

_Vulnerability / Penetration Testing Request on AWS not necessary_
Continuous Integration

Anytime You Need

SCAN

FIX

circleci

DETECT
Scan Methods
Scan Methods

- Multiple Databases

- OVAL: the Open Vulnerability and Assessment Language
- Security Advisory: RHSA/ALAS/ELSA/FreeBSD-SA
- Changelog: History of version changes
OVAL
(the Open Vulnerability and Assessment Language)

- Vulnerability information
  - Machine-processable XML format
  - https://oval.cisecurity.org/repository/registry
- Repositories
  - Debian (Debian Project)
  - Ubuntu (Canonical Ltd.)
  - RHEL (Red Hat, Inc.)
  - SUSE
  - Cisco (Cisco Systems, Inc.), etc.
Example (OVAL)

XML File / Security Update

<title>RHSA-2017:2485: git security update (important)</title>
<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>

<reference ref_id="CVE-2017-1000117" ... source="CVE"/>
CVE-2017-1000117

git is earlier than 0:1.7.1-9.el6_9
Version Definitions

- **Debian**
  - `deb-version`
  - Well-defined
  - [https://manpages.debian.org/jessie/dpkg-dev/deb-version.5.en.html](https://manpages.debian.org/jessie/dpkg-dev/deb-version.5.en.html)

- **Red Hat**
  - **Not found**
  - Read code and guess specifications
Sort versions from oldest to newest
(deb-version)
Old

`'~a'` < `'~a'` < `'~'` < `''` < `'1'` < `'10'` < `'a'`

New

deb-version
3.6.20-1.ab1 \leq 3.6.20-1.2

3.6.20-1.ab1 > 3.6.20-1.2

Debian

3.6.20-1.ab1 < 3.6.20-1.2

Red Hat
Compare Versions

- Sorting is “a bit” challenging
  - Complex sorting algorithm
  - (Old) ‘~~’ < ‘~~a’ < ‘~’ < ” < ‘a’ (New)

- Debian
  - 3.6.20-1.el6 > 3.6.20-1.2

- Red Hat
  - 3.6.20-1.el6 < 3.6.20-1.2

Opposite!
Security Advisories

- Security Information released by vendors (Red Hat, etc.)
- Advisory ID
- CVE-ID
- Synopsis, Severity, Description, Affected Products, Solution, etc.

<table>
<thead>
<tr>
<th>Advisory</th>
<th>Synopsis</th>
<th>Type / Severity</th>
<th>Products</th>
<th>Publish Date</th>
</tr>
</thead>
</table>
Security Advisories

- **Red Hat, Amazon Linux, Oracle Linux**
  - **How**
    - yum security plugin
  - **What**
    - RHSA (Red Hat Security Advisory)
    - ALAS (Amazon Linux AMI Security Advisory)
    - ELSA (Oracle Linux Security Advisories)

- **FreeBSD**
  - **How**
    - pkg-audit
  - **What**
    - FreeBSD-SA (FreeBSD Security Advisories)
$ sudo yum upgrade -s security

Loaded plugins: amazon-id, rhui-lb, search-disabled-repos
RHSA-2017:1680 Important/Sec. bind-libs-lite-32:9.9.4-50.el7_3.1.x86_64
RHBA-2017:2325 bugfix bind-libs-lite-32:9.9.4-51.el7.x86_64
RHSA-2017:1680 Important/Sec. bind-license-32:9.9.4-50.el7_3.1.noarch
RHBA-2017:2325 bugfix bind-license-32:9.9.4-51.el7.noarch
RHSA-2017:2473 Important/Sec. kernel-3.10.0-693.1.1.el7.x86_64
RHSA-2017:2473 Important/Sec. kernel-tools-3.10.0-693.1.1.el7.x86_64
RHSA-2017:2473 Important/Sec. kernel-tools-libs-3.10.0-693.1.1.el7.x86_64
RHBA-2017:2329 bugfix kmod-20-15.el7_4.1.x86_64
RHBA-2017:2329 bugfix kmod-libs-20-15.el7_4.1.x86_64
RHSA-2017:2473 Important/Sec. python-perf-3.10.0-693.1.1.el7.x86_64
Changelog

- History of version changes
- Relevant CVE ID is listed when a security issue is fixed.

### Bash (Red Hat)

* Mon Dec 12 12:00:00 2016 Siteshwar Vashisht <svashisht@redhat.com> - 4.1.2-47
  
  **CVE-2016-9401**: Fix crash when '-' is passed as second sign to `popd`
  
  Resolves: #1396383

* Mon Dec 12 12:00:00 2016 Siteshwar Vashisht <svashisht@redhat.com> - 4.1.2-46
  
  **CVE-2016-7543**: Fix for arbitrary code execution via `SHELLOPTS+PS4` variables
  
  Resolves: #1379630

* Mon Dec 12 12:00:00 2016 Siteshwar Vashisht <svashisht@redhat.com> - 4.1.2-45
  
  **CVE-2016-0634**: Fix for arbitrary code execution via malicious hostname
  
  Resolves: #1377613

* Fri Dec  9 12:00:00 2016 Siteshwar Vashisht <svashisht@redhat.com> - 4.1.2-44
  
  - Avoid crash in parameter expansion while expanding long strings
  
  Resolves: #1359142
# Bash (Red Hat)

<table>
<thead>
<tr>
<th>FIXED CVE-ID</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2016-9401</td>
<td>4.1.2-47</td>
</tr>
<tr>
<td>CVE-2016-7543</td>
<td>4.1.2-46</td>
</tr>
<tr>
<td>CVE-2016-0634</td>
<td>4.1.2-45</td>
</tr>
<tr>
<td>_</td>
<td>4.1.2-44</td>
</tr>
</tbody>
</table>

- **Newest version**: 4.1.2-47
- **Currently installed version**: 4.1.2-44
Unique Features

- Execute commands on the server
  - Detect processes which needs restart after update
    - Debian
      - checkrestart
    - Red Hat
      - needs-restarting

<table>
<thead>
<tr>
<th>PID</th>
<th>Process</th>
<th>Restart required</th>
</tr>
</thead>
<tbody>
<tr>
<td>432</td>
<td>ntpd</td>
<td></td>
</tr>
<tr>
<td>930</td>
<td>sshd</td>
<td></td>
</tr>
<tr>
<td>1157</td>
<td>httpd</td>
<td></td>
</tr>
</tbody>
</table>
Features In The Future

- Detect vulnerabilities for which there’s no update yet
- Monitor Security Trackers (Debian, Ubuntu, Red Hat, etc)

CVE-2016-8615

<table>
<thead>
<tr>
<th>Affected Packages State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
</tr>
<tr>
<td>Red Hat JBoss Web Server 3.0</td>
</tr>
<tr>
<td>Red Hat JBoss Core Services 1</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 7</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 6</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5</td>
</tr>
<tr>
<td>RHEV-M for Servers</td>
</tr>
<tr>
<td>State</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>Fix deferred</td>
</tr>
<tr>
<td>Affected</td>
</tr>
<tr>
<td>Will not fix</td>
</tr>
<tr>
<td>Will not fix</td>
</tr>
<tr>
<td>Will not fix</td>
</tr>
<tr>
<td>Affected</td>
</tr>
</tbody>
</table>

- **No update yet**
- **Will not fix**
- **No update yet**
Features In The Future

- Find Exploit Code (PoC)
  - The Exploit Database, Metasploit, etc.
Vuls SaaS

- Supports the workflow in later phases
  - Assign tasks to members
  - Set deadline for fixing vulnerabilities
- Re-calculate CVSS score based on your environment
Summary

Fast
High-quality
Extensive OS Support

On-Premise and Cloud
Flexible
Thank you for your time!

kotakanbe@gmail.com
knqyf263@gmail.com