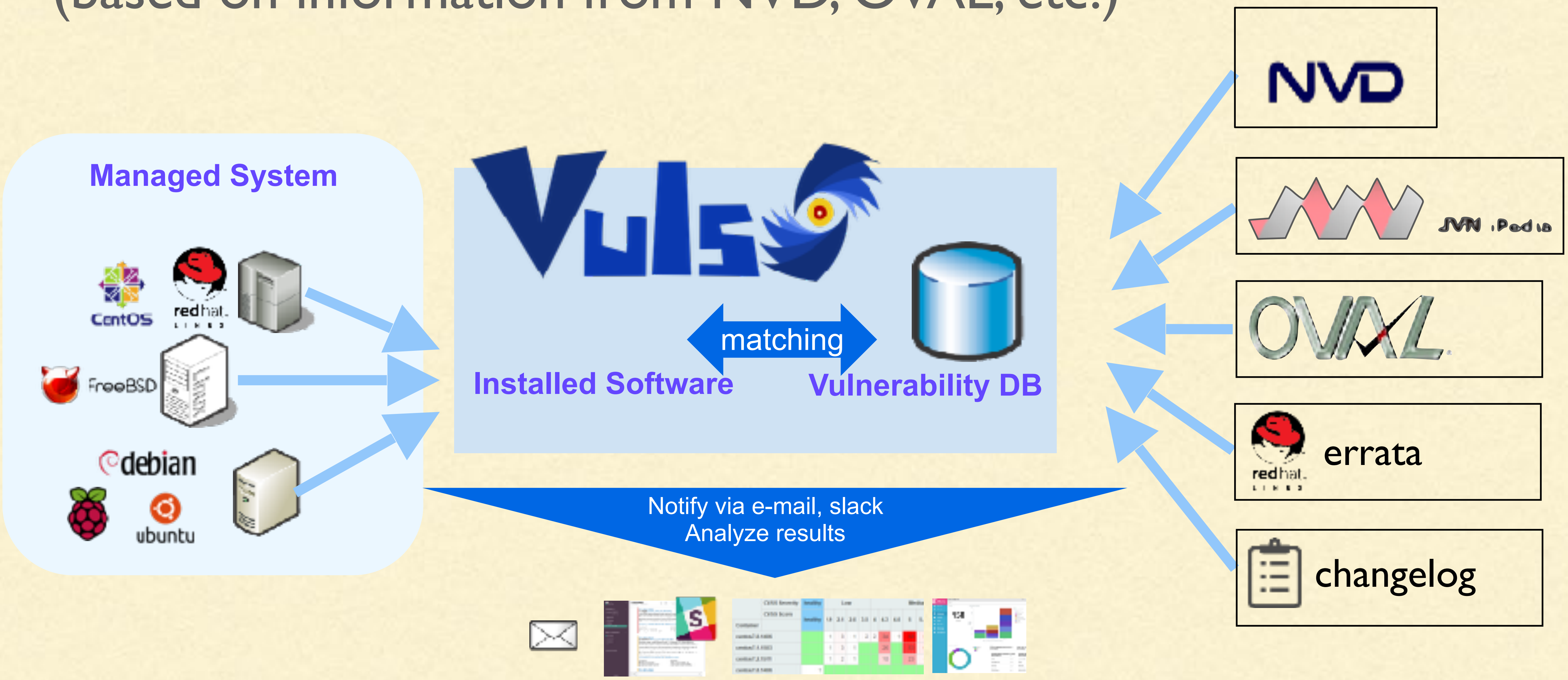
Automating Vulnerability Assessments with Vuls

Kota KANBE & Teppei FUKUDA

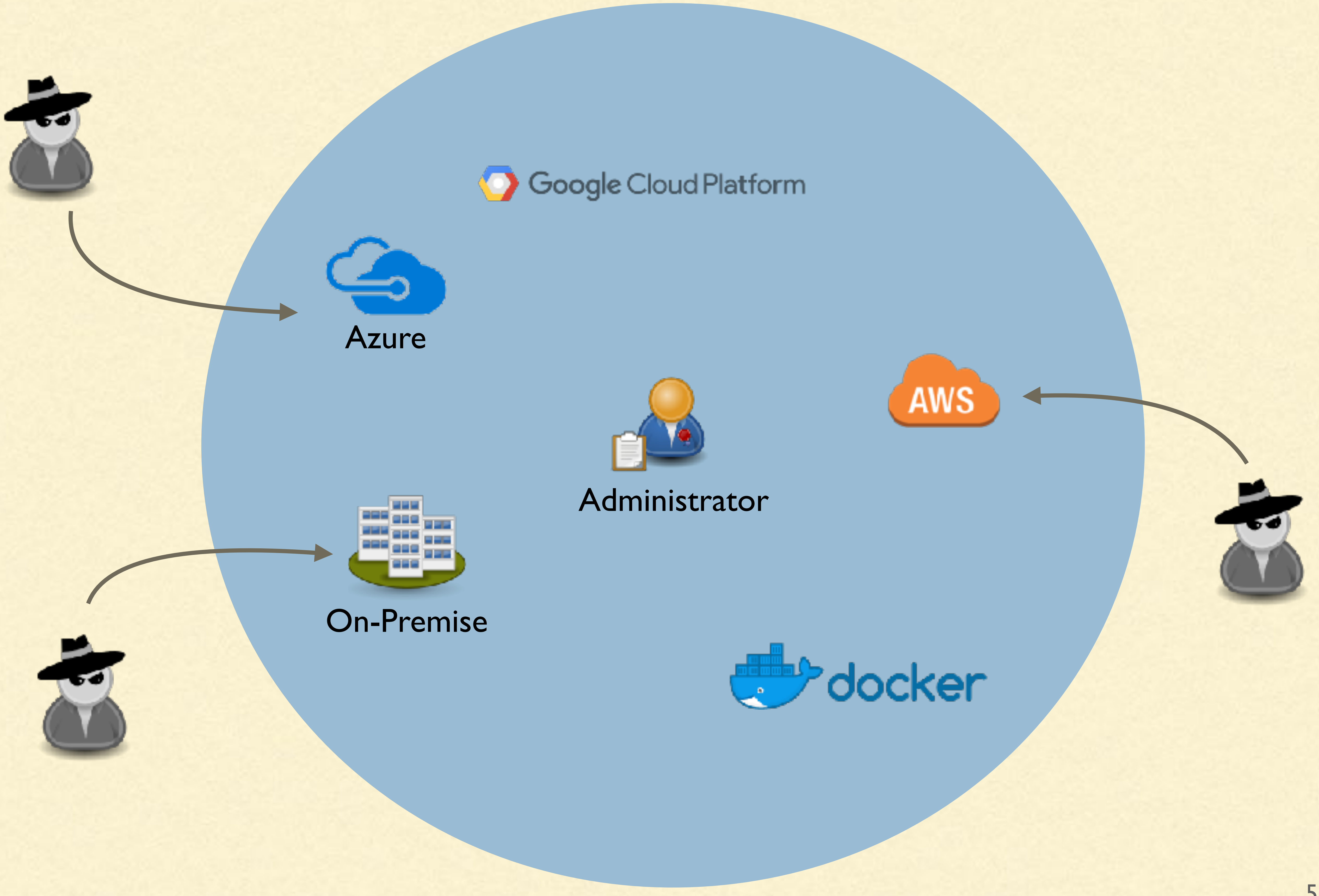
HITCON CMT 2017

Vuls

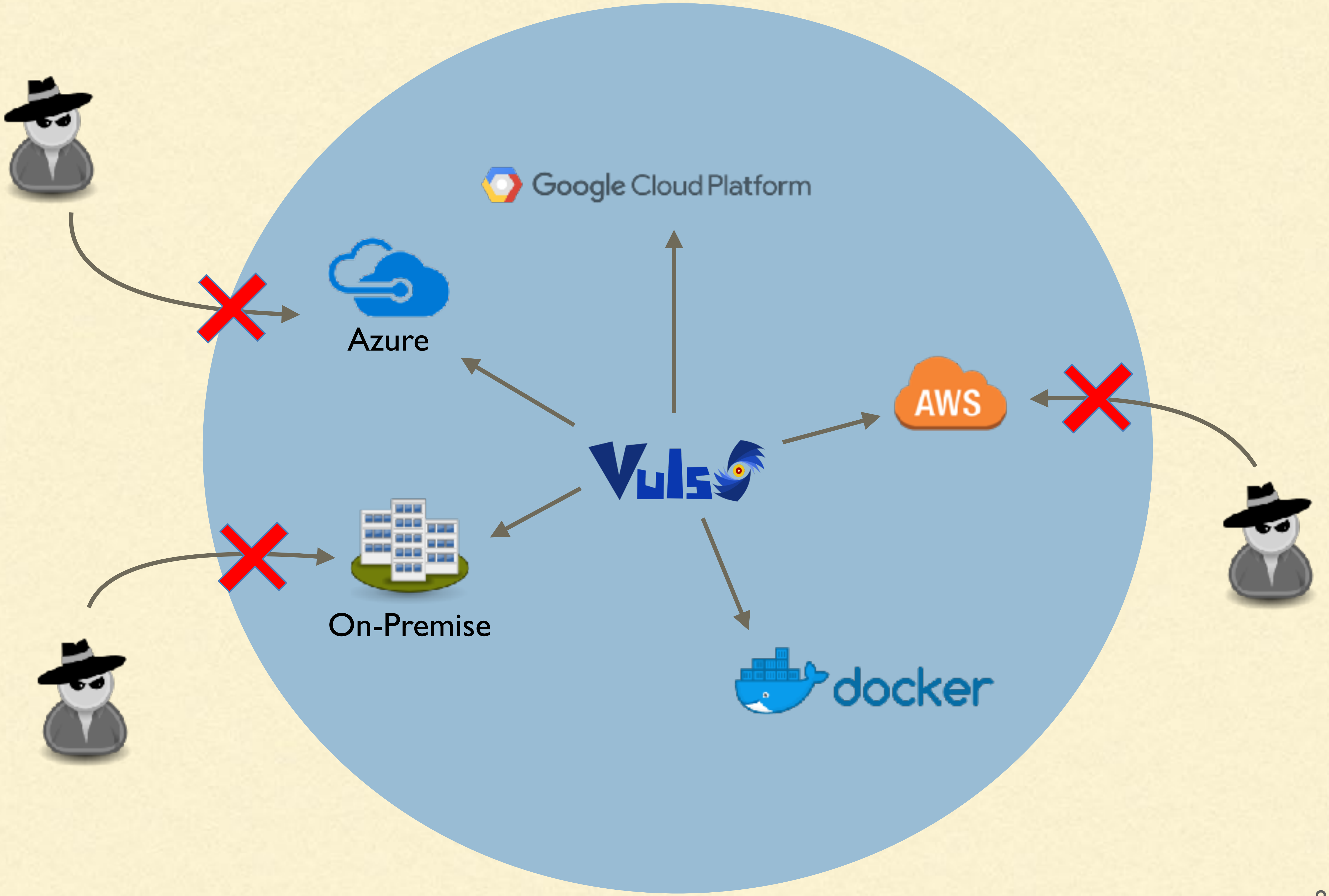
- open-source, agent-less vulnerability scanner (based on information from NVD, OVAL, etc.)

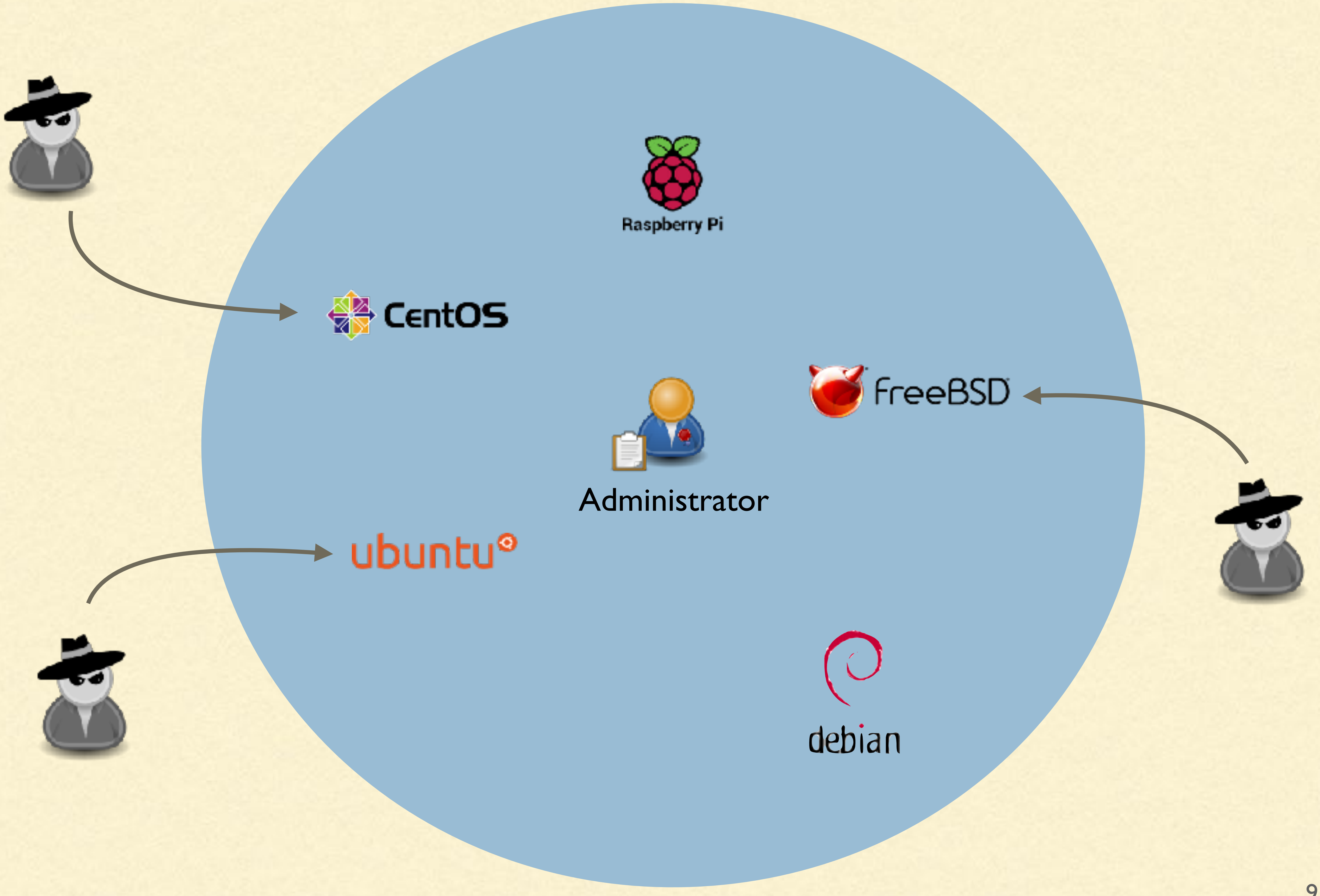


Vuls Features In-Depth

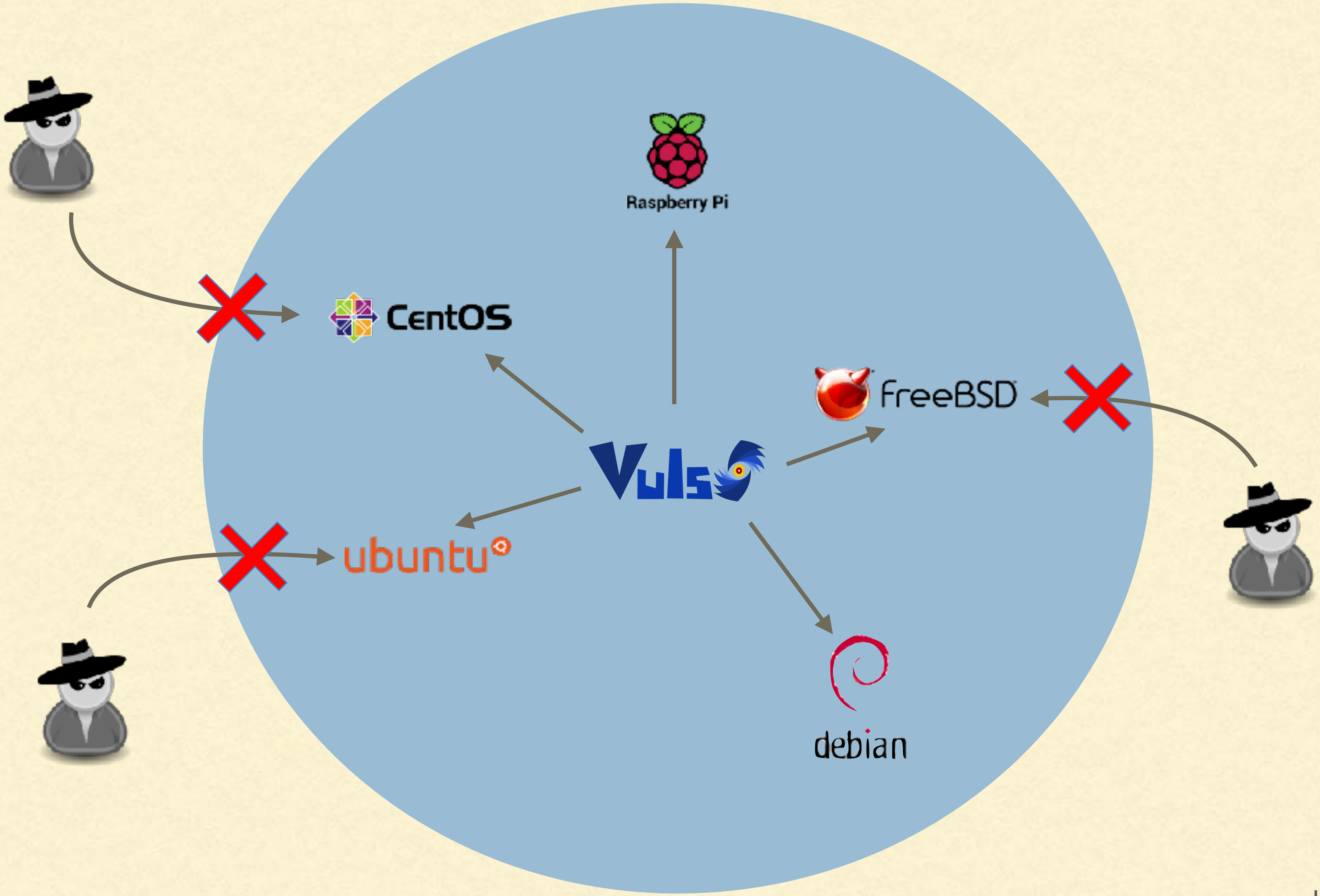

Google Cloud Platform
Azure
AWS
Administrator
On-Premise
docker

Vuls


Google Cloud Platform
Azure
AWS
Vuls
On-Premise
docker

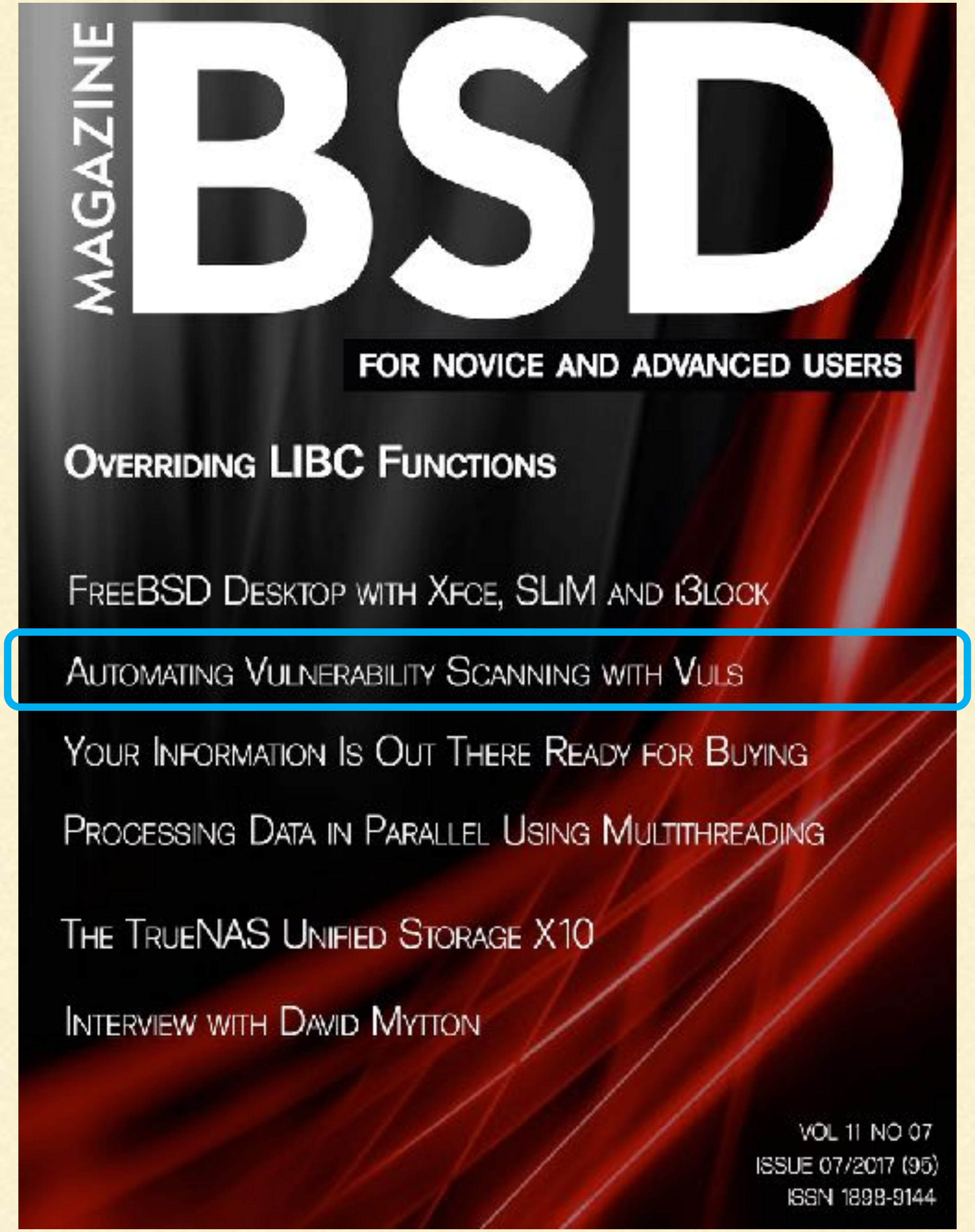

Raspberry Pi
CentOS
FreeBSD
Administrator
ubuntu
debian

Vuls


Raspberry Pi
CentOS
FreeBSD
Vuls
ubuntu
debian

Supported OS

Ubuntu	12, 14, 16
Debian	7, 8, 9
RHEL	5, 6, 7
Oracle Linux	5, 6, 7
CentOS	6, 7
Amazon Linux	All
FreeBSD	10, 11
Raspbian	Jessie, Stretch



MAGAZINE

BSD

FOR NOVICE AND ADVANCED USERS

Overriding LIBC Functions

FreeBSD Desktop with Xfce, SLiM and i3Lock

Automating Vulnerability Scanning with Vuls

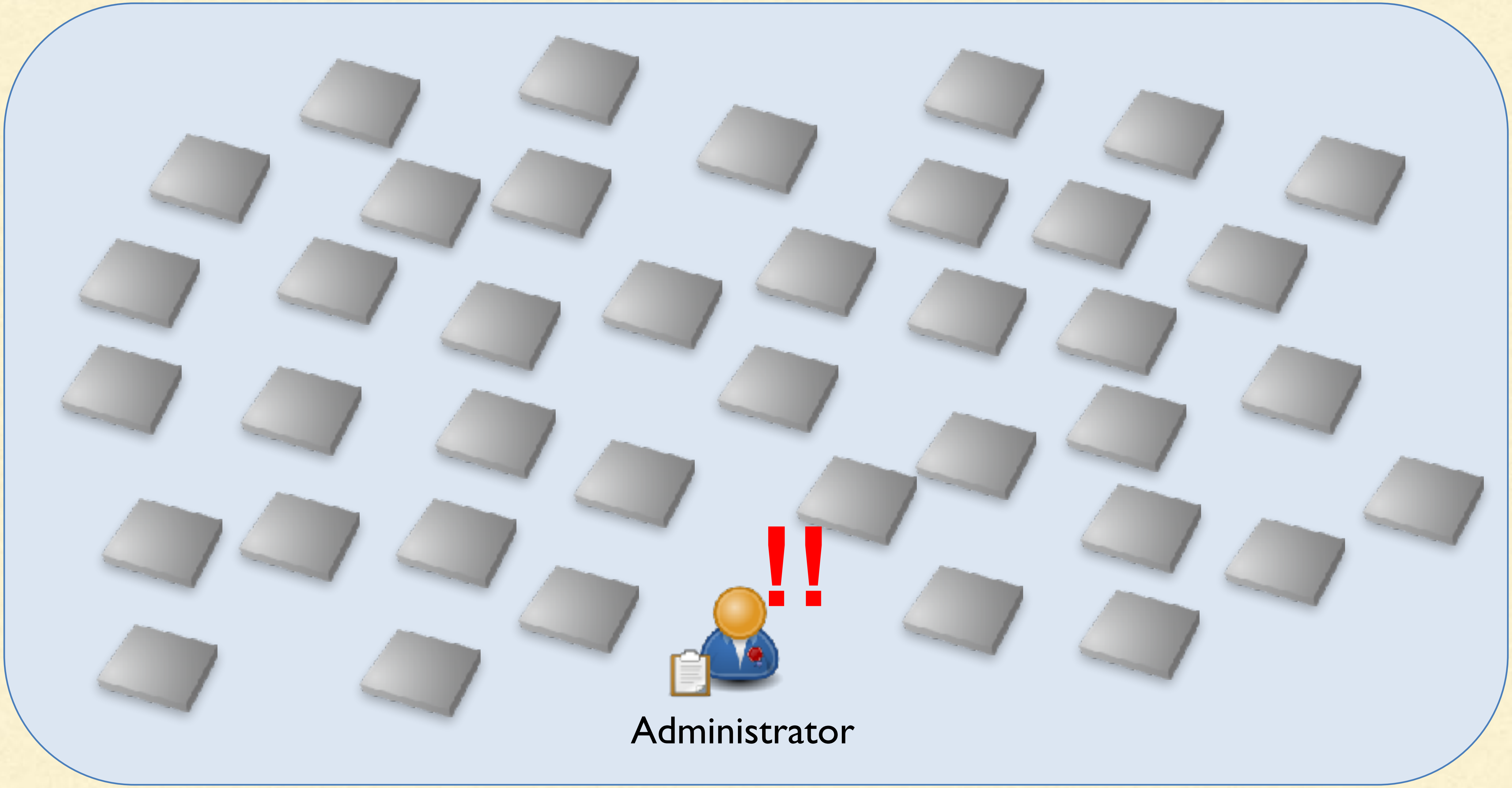
Your Information Is Out There Ready for Buying

Processing Data in Parallel Using Multithreading

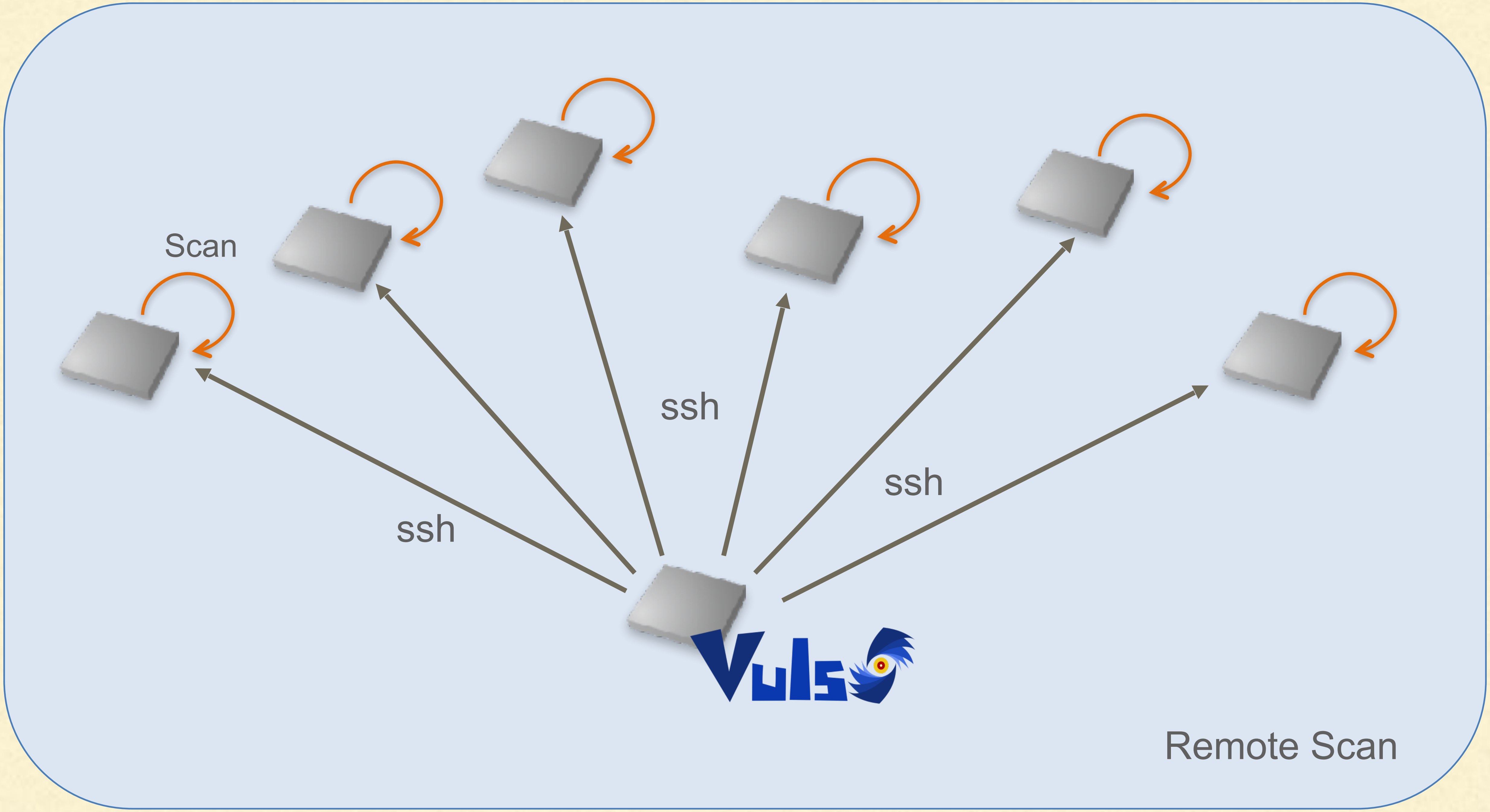
The TrueNAS Unified Storage X10

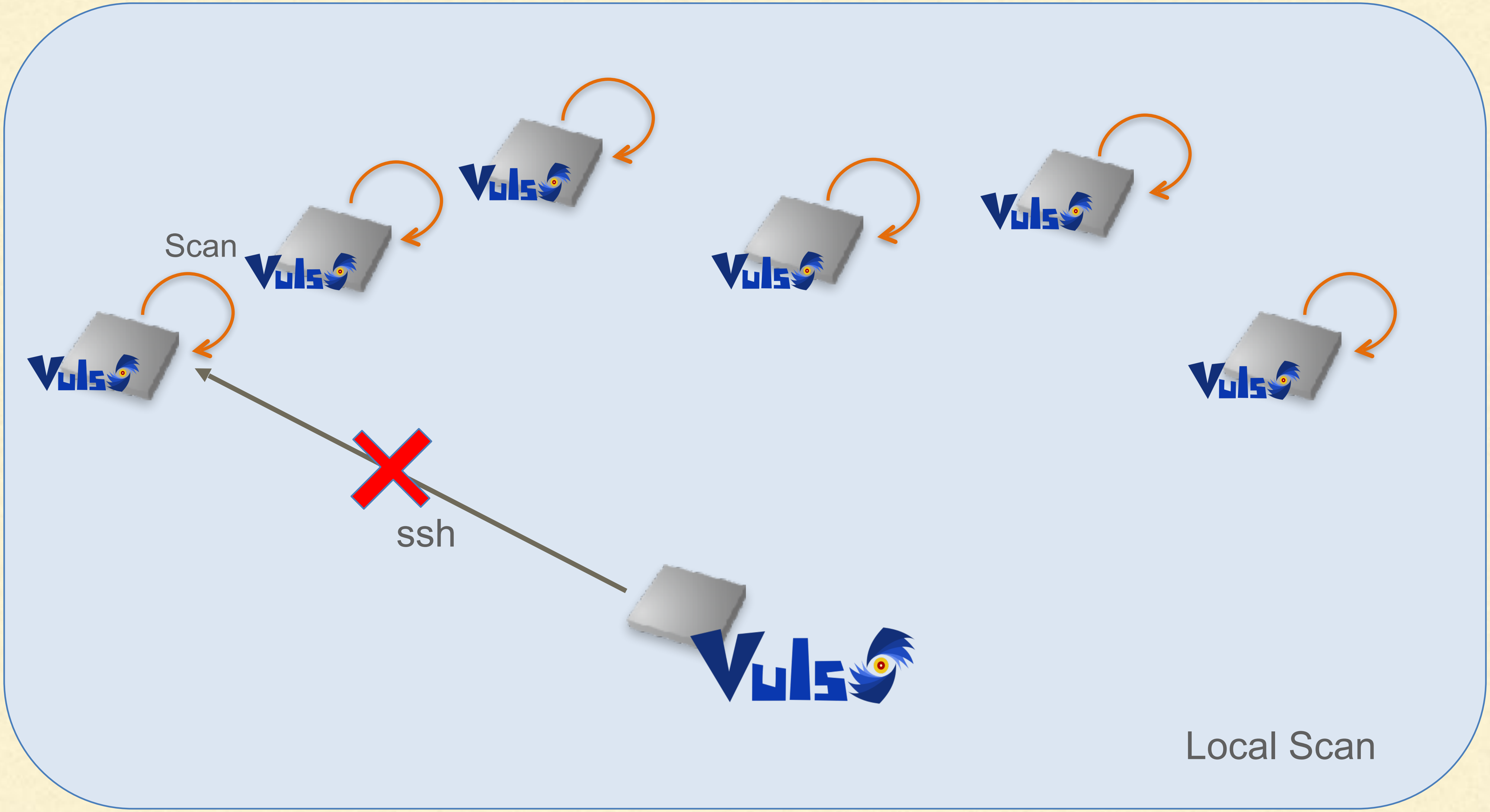
Interview with David Mytton

VOL 11 NO 07
ISSUE 07/2017 (95)
ISSN 1898-9144


!!
Administrator

Agent-less

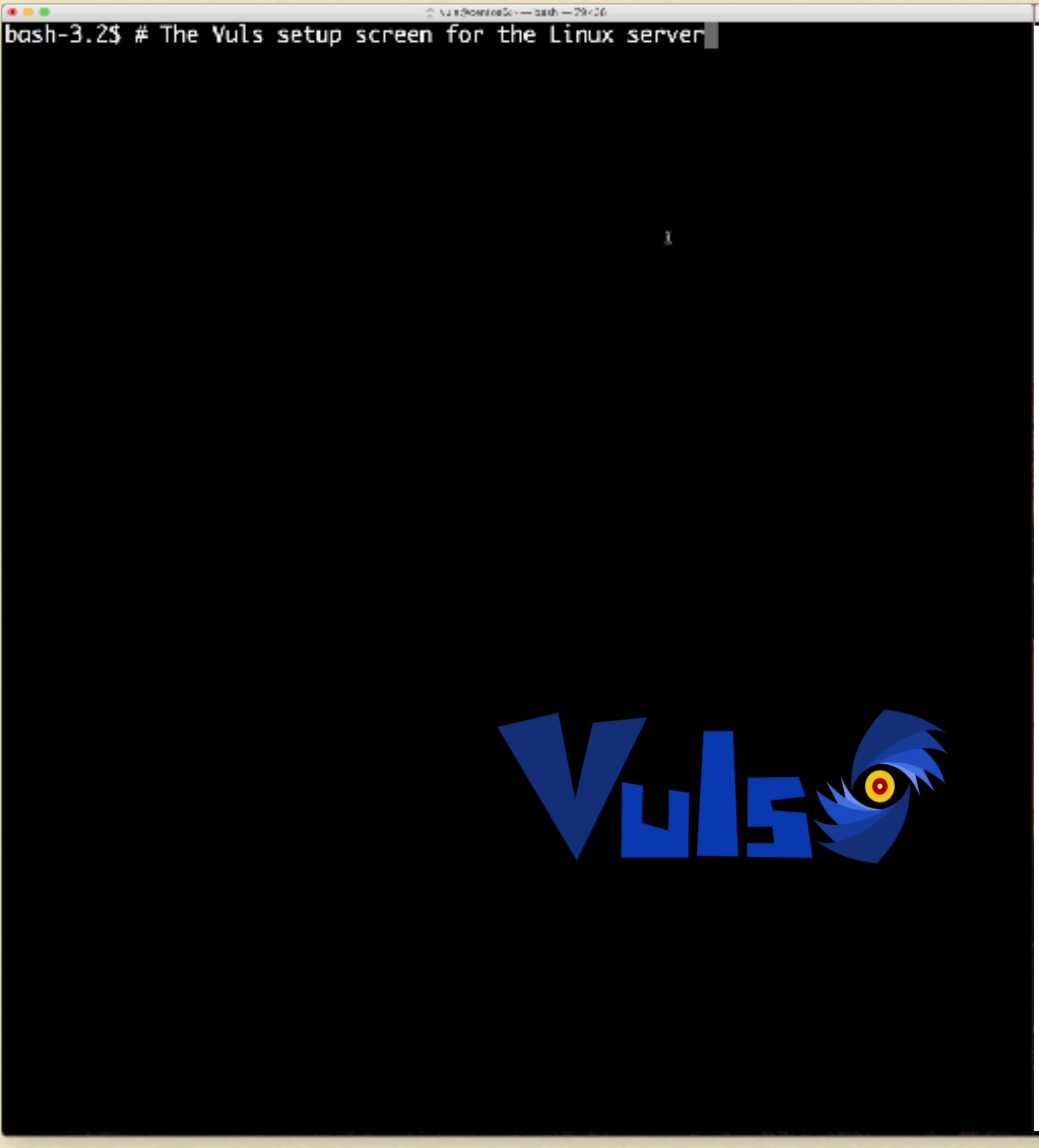

Scan
ssh
ssh
ssh
Vuls
Remote Scan


Scan
ssh
Local Scan

DEMO

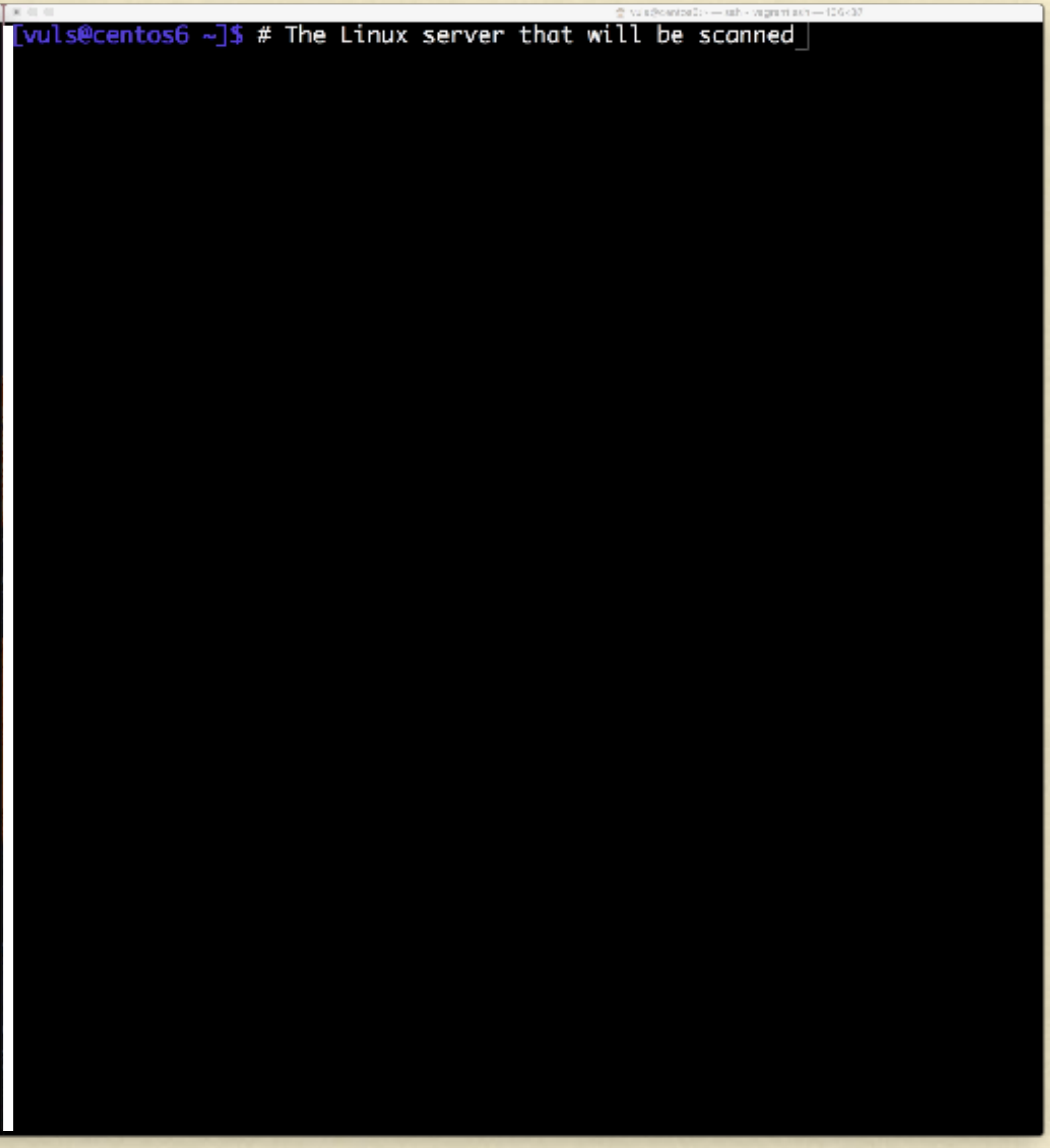
Let’s see just how easy it is to use Vuls

Vuls setup screen for the Linux server



```
bash-3.2$ # The Vuls setup screen for the Linux server
```

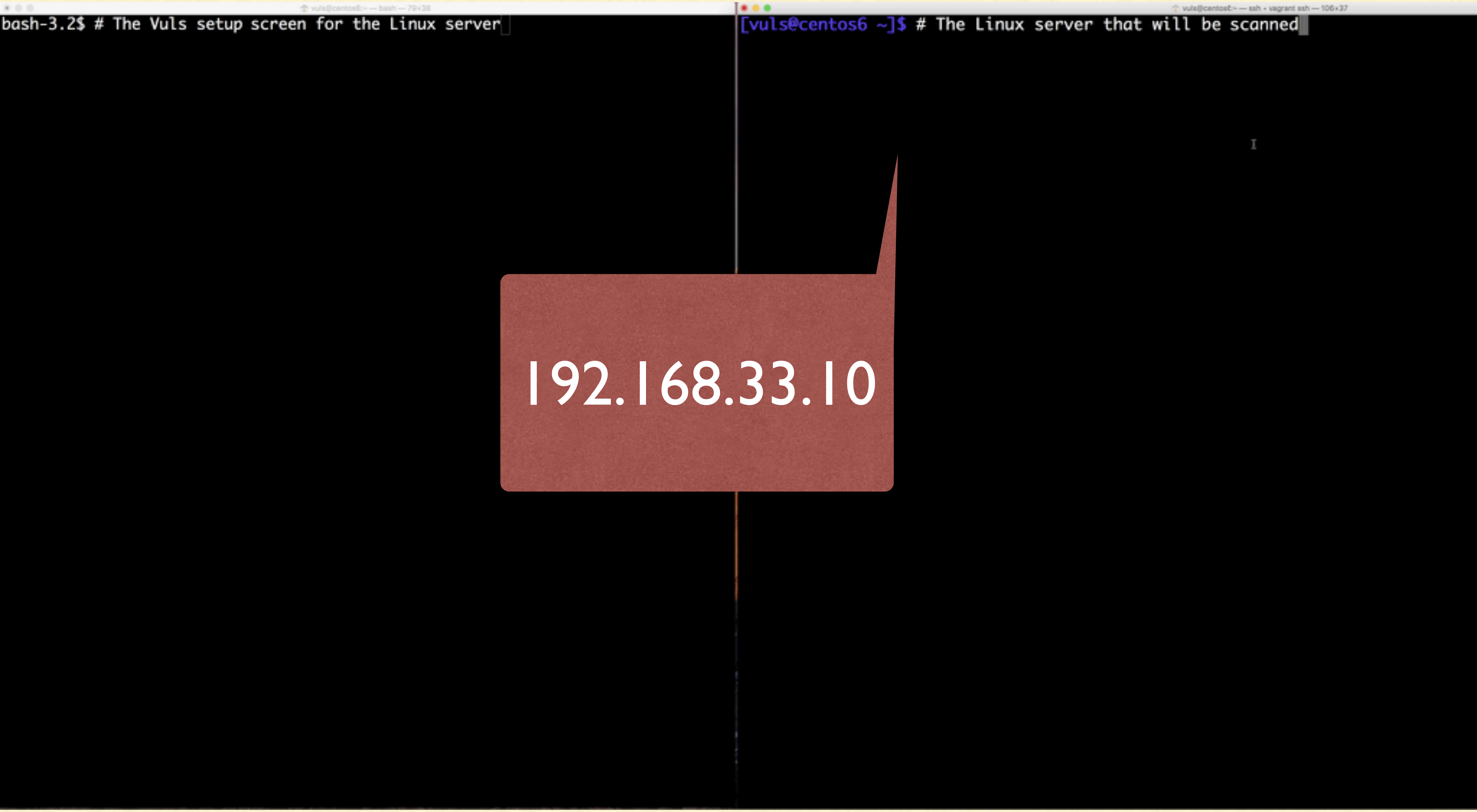
Linux server that will be scanned



```
[vuls@centos6 ~]$ # The Linux server that will be scanned
```

Vuls setup server

Linux server that will be scanned



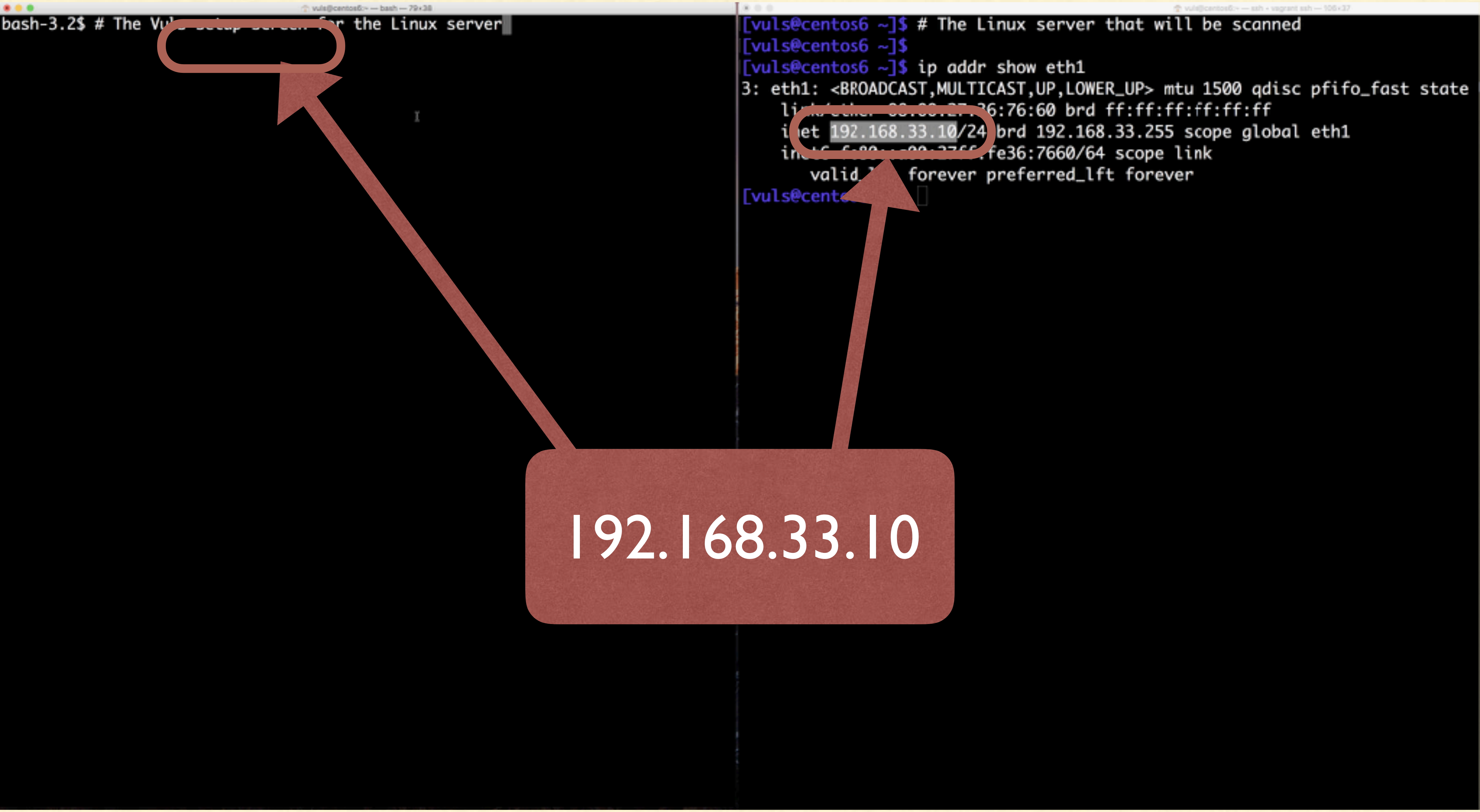
```
bash-3.2$ # The Vuls setup screen for the Linux server
```

```
[vuls@centos6 ~]$ # The Linux server that will be scanned
```

192.168.33.10

Vuls setup server

Linux server
that will be scanned



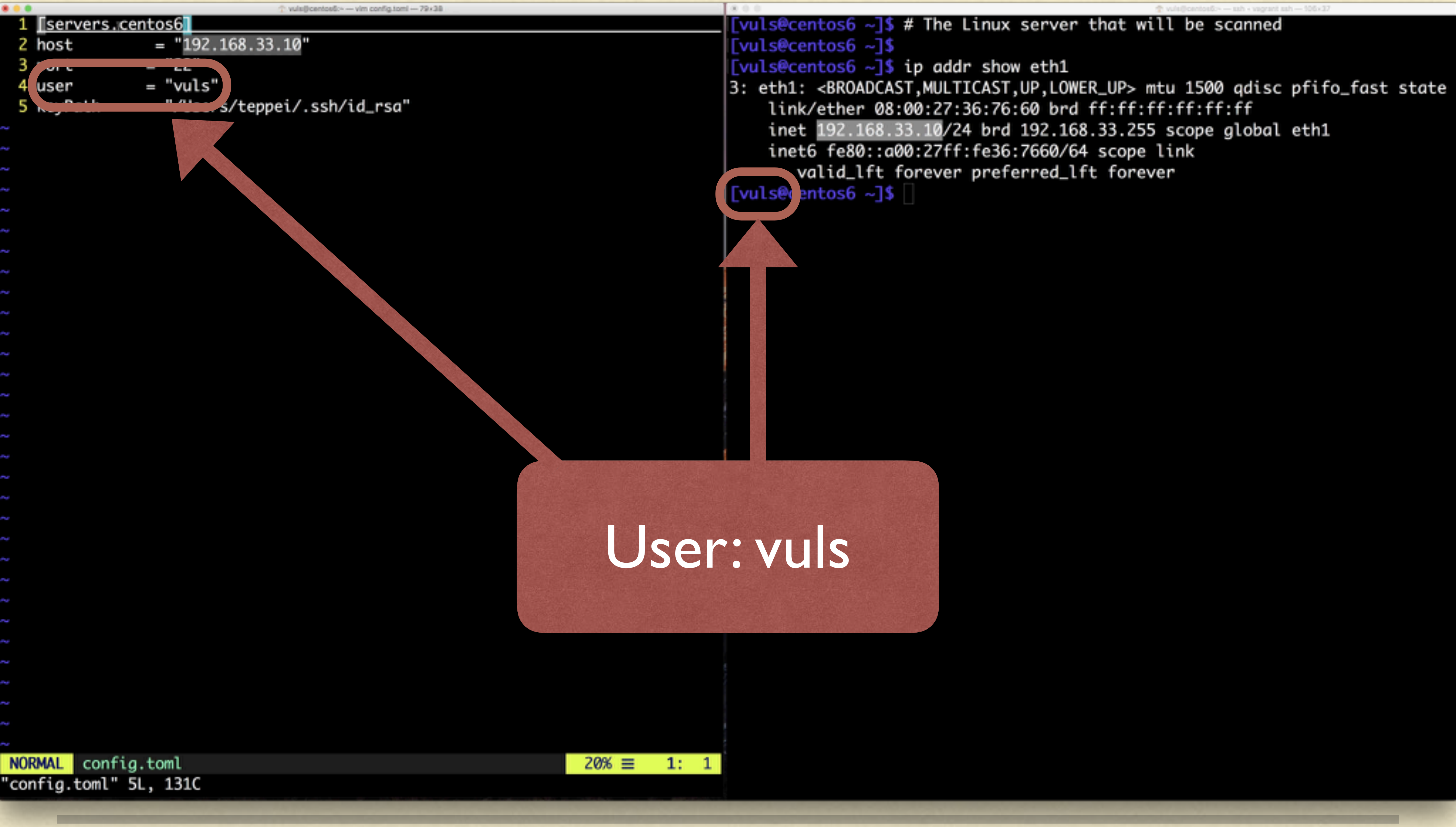
```
bash-3.2$ # The Vuls setup screen for the Linux server
```

```
[vuls@centos6 ~]$ # The Linux server that will be scanned
[vuls@centos6 ~]$
[vuls@centos6 ~]$ ip addr show eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
    link/ether 08:00:27:36:76:60 brd ff:ff:ff:ff:ff:ff
    inet 192.168.33.10/24 brd 192.168.33.255 scope global eth1
    inet6 fe80::a00:27ff:fe36:7660/64 scope link
       valid_lft forever preferred_lft forever
[vuls@centos6 ~]$
```

192.168.33.10

Vuls setup server

Linux server that will be scanned

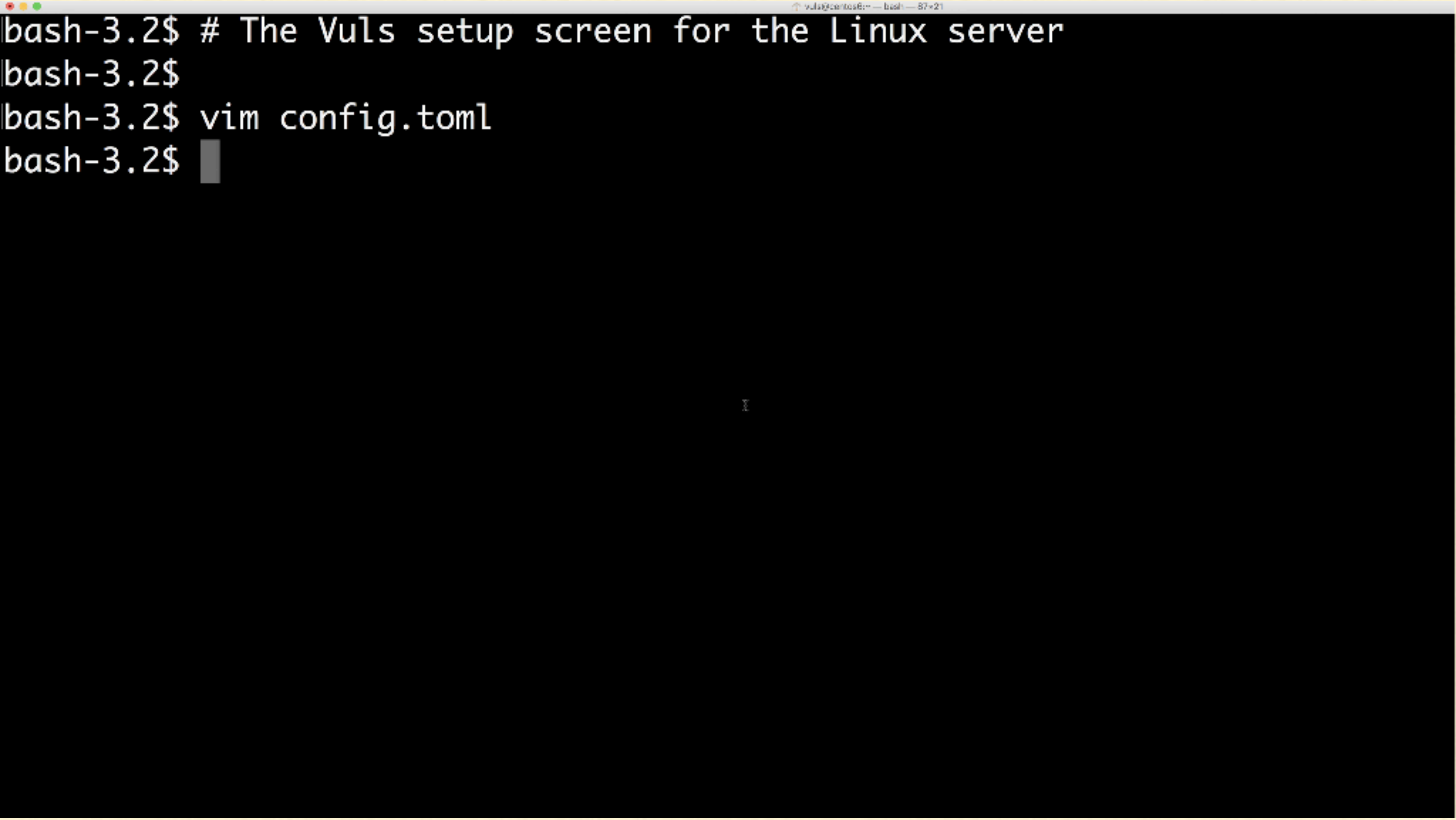


```
[servers.centos6]
host         = "192.168.33.10"
port        = "22"
user        = "vuls"
keyPath     = "/Users/teppei/.ssh/id_rsa"
~
NORMAL  config.toml                                              20% ≡   1:  1
"config.toml" 5L, 131C
```

```
[vuls@centos6 ~]$ # The Linux server that will be scanned
[vuls@centos6 ~]$
[vuls@centos6 ~]$ ip addr show eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
    link/ether 08:00:27:36:76:60 brd ff:ff:ff:ff:ff:ff
    inet 192.168.33.10/24 brd 192.168.33.255 scope global eth1
    inet6 fe80::a00:27ff:fe36:7660/64 scope link
       valid_lft forever preferred_lft forever
[vuls@centos6 ~]$
```

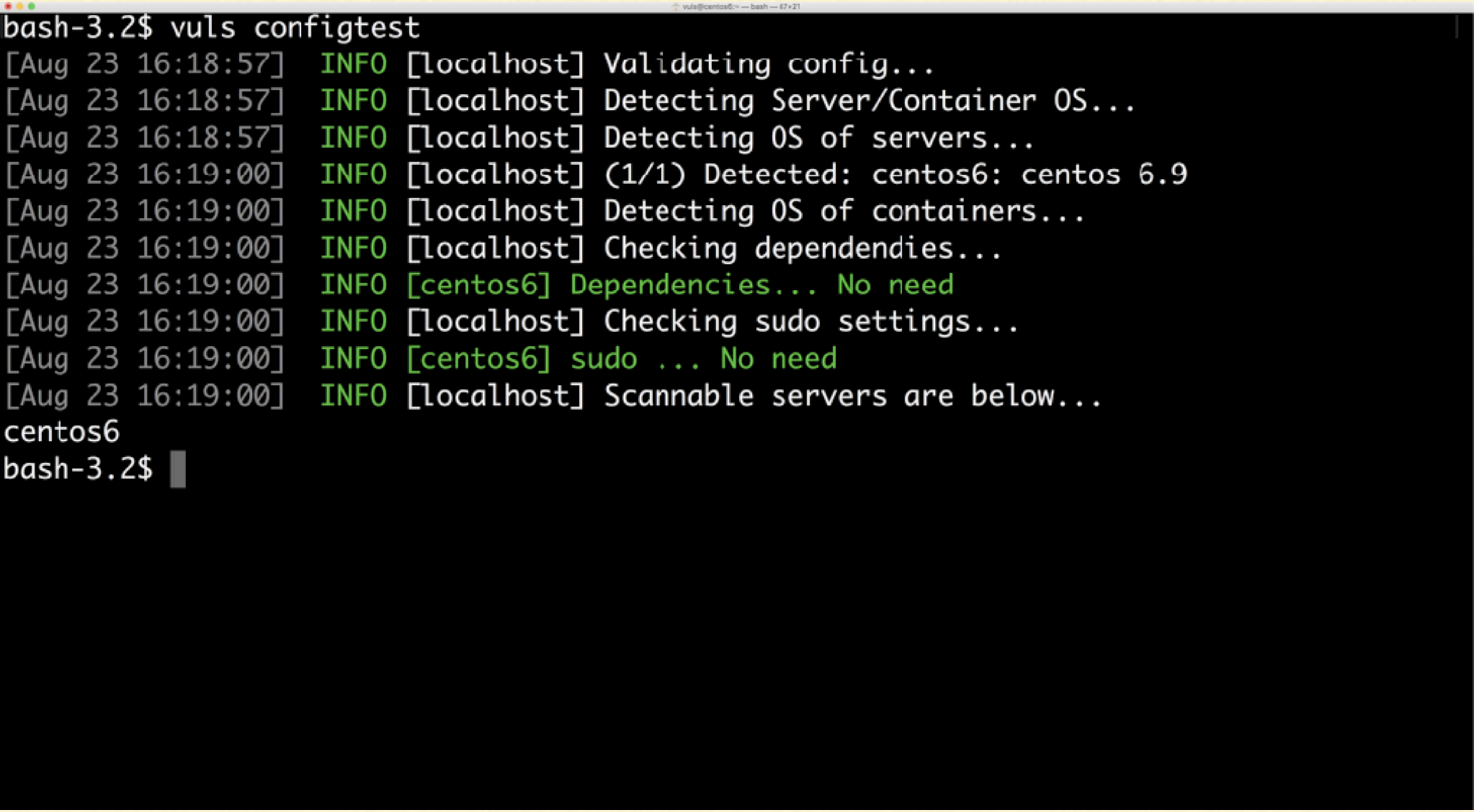
User: vuls

Vuls setup server



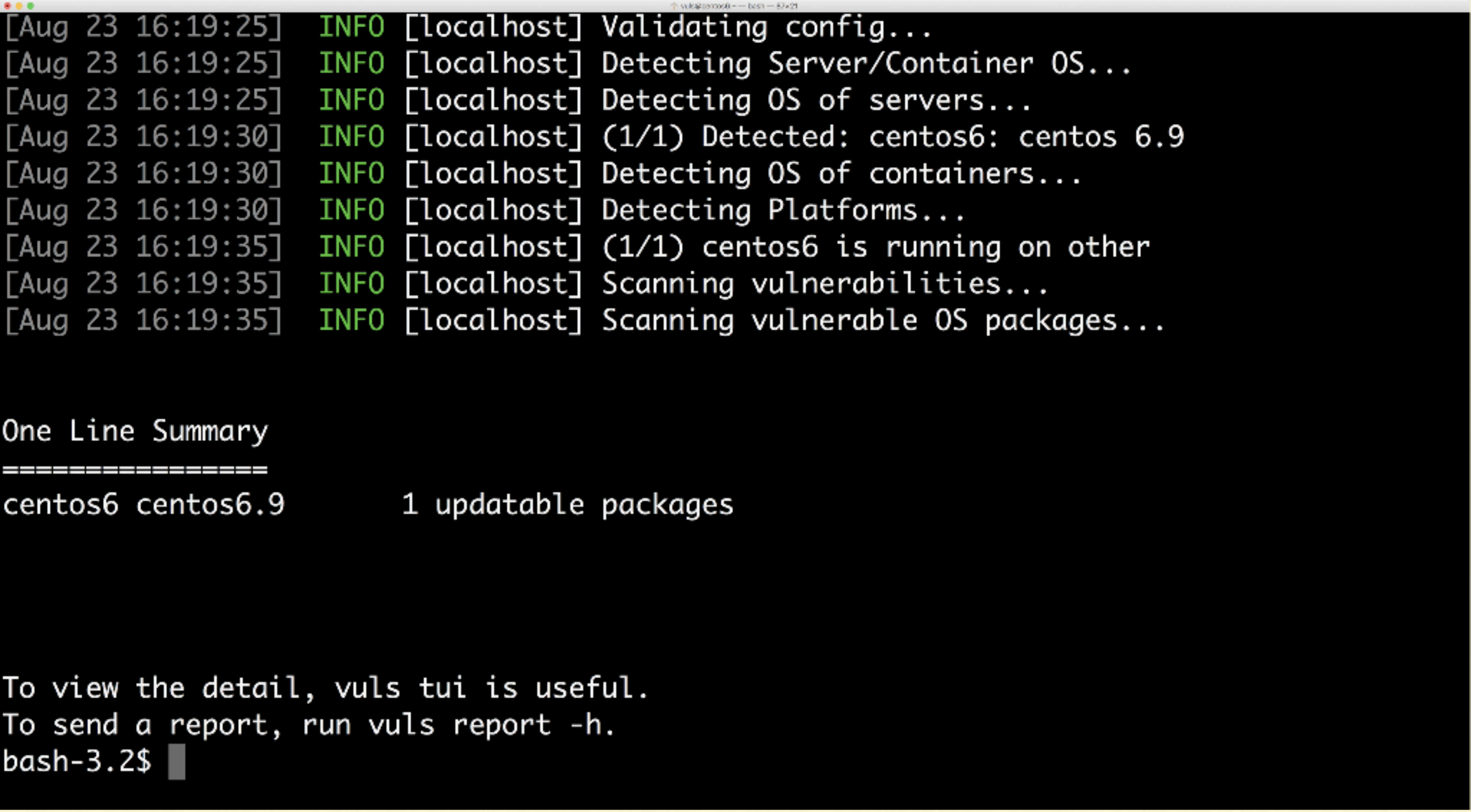
```
bash-3.2$ # The Vuls setup screen for the Linux server
bash-3.2$
bash-3.2$ vim config.toml
bash-3.2$
```

Scan



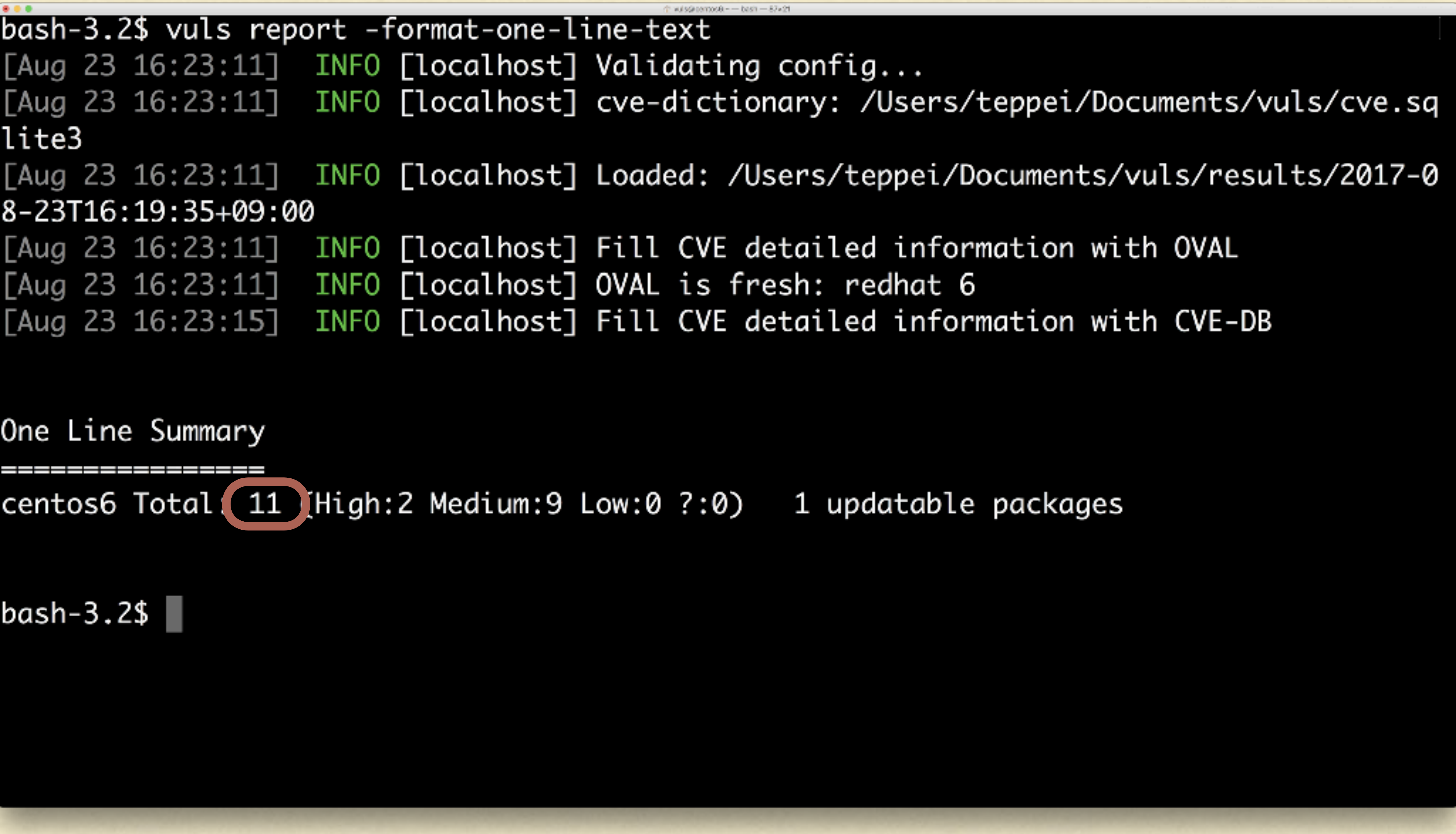
```
bash-3.2$ vuls configtest
[Aug 23 16:18:57]  INFO [localhost] Validating config...
[Aug 23 16:18:57]  INFO [localhost] Detecting Server/Container OS...
[Aug 23 16:18:57]  INFO [localhost] Detecting OS of servers...
[Aug 23 16:19:00]  INFO [localhost] (1/1) Detected: centos6: centos 6.9
[Aug 23 16:19:00]  INFO [localhost] Detecting OS of containers...
[Aug 23 16:19:00]  INFO [localhost] Checking dependendies...
[Aug 23 16:19:00]  INFO [centos6] Dependencies... No need
[Aug 23 16:19:00]  INFO [localhost] Checking sudo settings...
[Aug 23 16:19:00]  INFO [centos6] sudo ... No need
[Aug 23 16:19:00]  INFO [localhost] Scannable servers are below...
centos6
bash-3.2$ 
```

Report



```
[Aug 23 16:19:25]  INFO [localhost] Validating config...
[Aug 23 16:19:25]  INFO [localhost] Detecting Server/Container OS...
[Aug 23 16:19:25]  INFO [localhost] Detecting OS of servers...
[Aug 23 16:19:30]  INFO [localhost] (1/1) Detected: centos6: centos 6.9
[Aug 23 16:19:30]  INFO [localhost] Detecting OS of containers...
[Aug 23 16:19:30]  INFO [localhost] Detecting Platforms...
[Aug 23 16:19:35]  INFO [localhost] (1/1) centos6 is running on other
[Aug 23 16:19:35]  INFO [localhost] Scanning vulnerabilities...
[Aug 23 16:19:35]  INFO [localhost] Scanning vulnerable OS packages...


One Line Summary
================
centos6 centos6.9       1 updatable packages




To view the detail, vuls tui is useful.
To send a report, run vuls report -h.
bash-3.2$ 
```

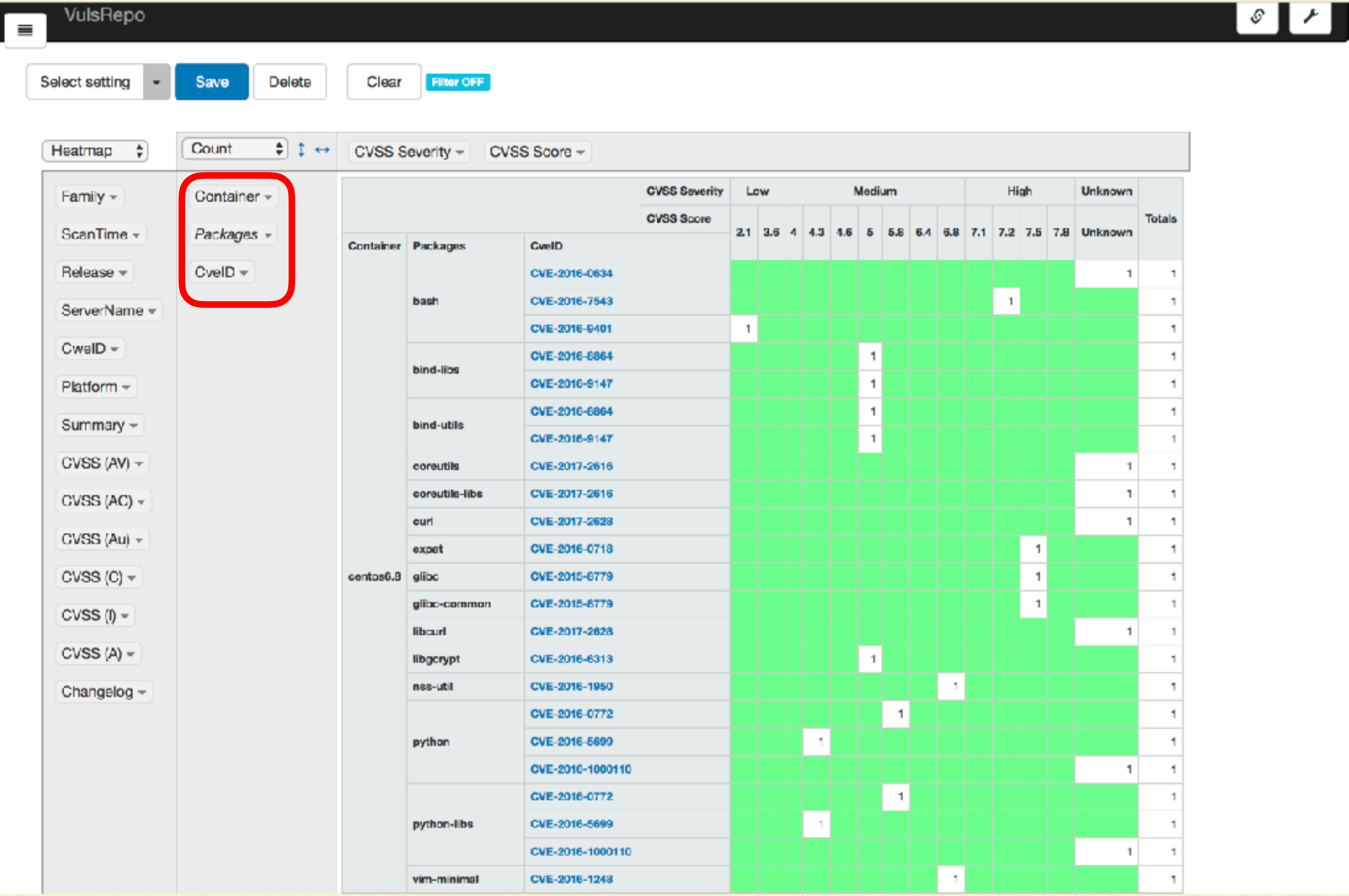
Report



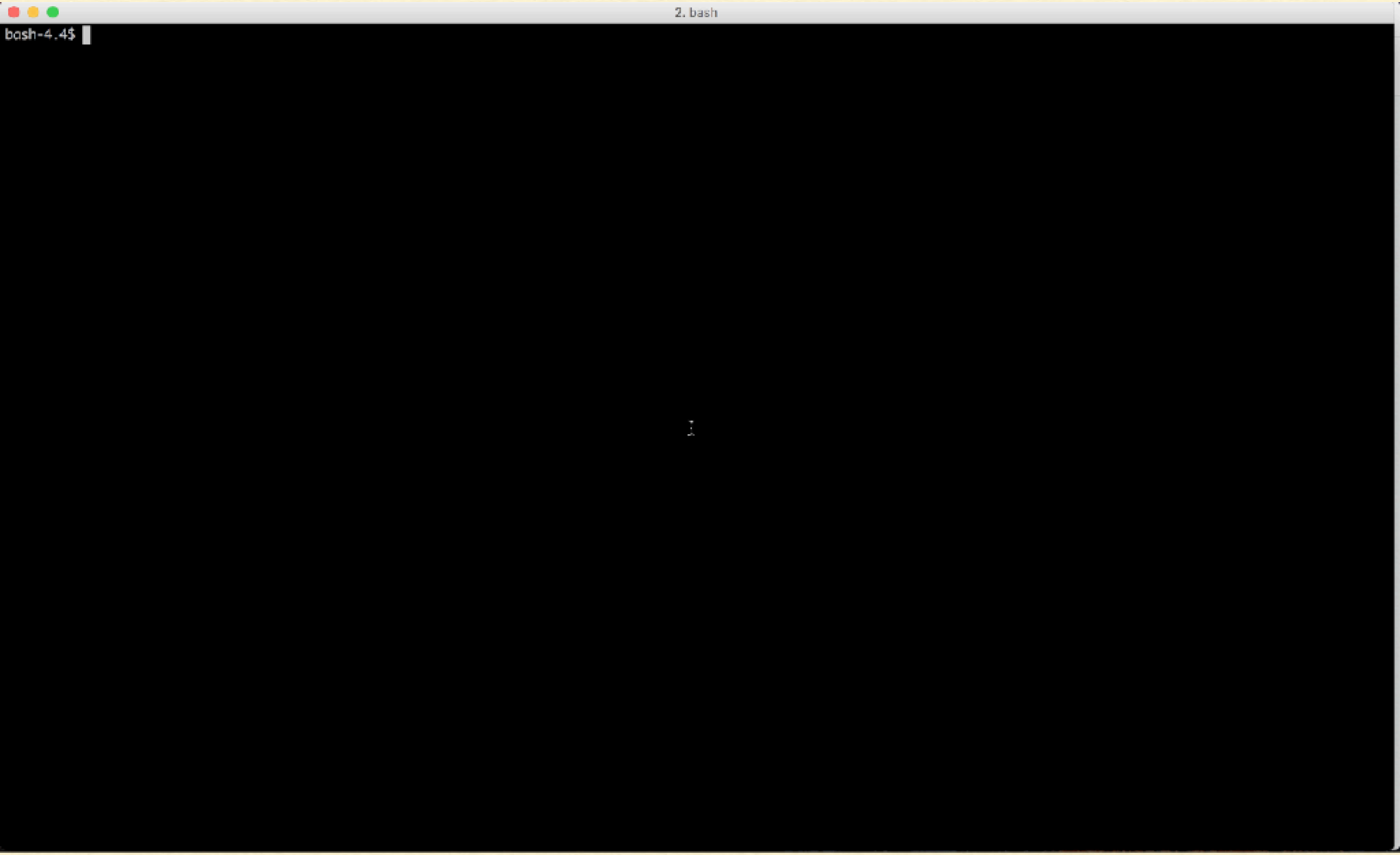
```
bash-3.2$ vuls report -format-one-line-text
[Aug 23 16:23:11]  INFO [localhost] Validating config...
[Aug 23 16:23:11]  INFO [localhost] cve-dictionary: /Users/teppei/Documents/vuls/cve.sq
lite3
[Aug 23 16:23:11]  INFO [localhost] Loaded: /Users/teppei/Documents/vuls/results/2017-0
8-23T16:19:35+09:00
[Aug 23 16:23:11]  INFO [localhost] Fill CVE detailed information with OVAL
[Aug 23 16:23:11]  INFO [localhost] OVAL is fresh: redhat 6
[Aug 23 16:23:15]  INFO [localhost] Fill CVE detailed information with CVE-DB


One Line Summary
================
centos6 Total: 11 (High:2 Medium:9 Low:0 ?:0)   1 updatable packages


bash-3.2$
```

Check the Scan Results

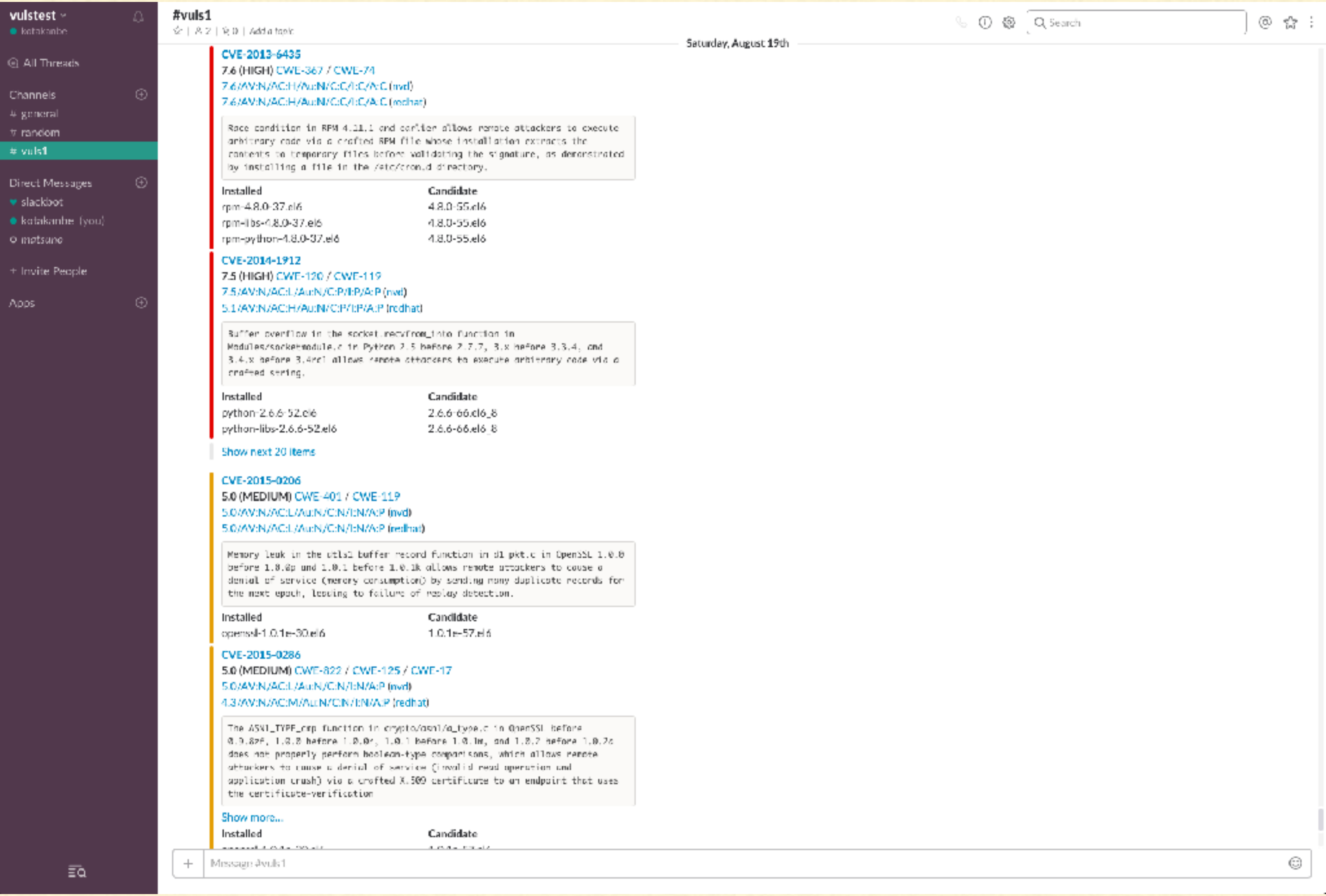
- View results with
  - VulsRepo (OSS)
  - TUI (Text-based User Interface)
- Get notifications of results by
  - E-mail
  - Slack



		CVSS Severity	Low	Medium							High				Unknown	Totals
		CVSS Score	2.1	3.6	4	4.3	4.6	5	5.8	6.4	6.8	7.1	7.2	7.5	7.8	Unknown	
Container	Packages	CveID															
centos6.8	bash	CVE-2016-0634														1	1
		CVE-2016-7543											1				1
		CVE-2016-9401	1														1
	bind-libs	CVE-2016-8864						1									1
		CVE-2016-9147						1									1
	bind-utils	CVE-2016-8864						1									1
		CVE-2016-9147						1									1
	coreutils	CVE-2017-2616														1	1
	coreutils-libs	CVE-2017-2616														1	1
	curl	CVE-2017-2628														1	1
	expat	CVE-2016-0718												1			1
	glibc	CVE-2015-8779												1			1
	glibc-common	CVE-2015-8779												1			1
	libcurl	CVE-2017-2628														1	1
	libgcrypt	CVE-2016-6313						1									1
	nss-util	CVE-2016-1950									1						1
	python	CVE-2016-0772							1								1
		CVE-2016-5699				1											1
		CVE-2016-1000110														1	1
	python-libs	CVE-2016-0772							1								1
		CVE-2016-5699				1											1
		CVE-2016-1000110														1	1
	vim-minimal	CVE-2016-1248									1						1



```
bash-4.4$
```



Saturday, August 19th

CVE-2013-6435
7.6 (HIGH) CWE-367 / CWE-74
7.6/AV:N/AC:H/Au:N/C:C/I:C/A:C (nvd)
7.6/AV:N/AC:H/Au:N/C:C/I:C/A:C (redhat)

```
Race condition in RPM 4.11.1 and earlier allows remote attackers to execute
arbitrary code via a crafted RPM file whose installation extracts the
contents to temporary files before validating the signature, as demonstrated
by installing a file in the /etc/cron.d directory.
```

Installed	Candidate
rpm-4.8.0-37.el6	4.8.0-55.el6
rpm-libs-4.8.0-37.el6	4.8.0-55.el6
rpm-python-4.8.0-37.el6	4.8.0-55.el6

CVE-2014-1912
7.5 (HIGH) CWE-120 / CWE-119
7.5/AV:N/AC:L/Au:N/C:P/I:P/A:P (nvd)
5.1/AV:N/AC:H/Au:N/C:P/I:P/A:P (redhat)

```
Buffer overflow in the socket.recvfrom_into function in
Modules/socketmodule.c in Python 2.5 before 2.7.7, 3.x before 3.3.4, and
3.4.x before 3.4rc1 allows remote attackers to execute arbitrary code via a
crafted string.
```

Installed	Candidate
python-2.6.6-52.el6	2.6.6-66.el6_8
python-libs-2.6.6-52.el6	2.6.6-66.el6_8

Show next 20 items

CVE-2015-0206
5.0 (MEDIUM) CWE-401 / CWE-119
5.0/AV:N/AC:L/Au:N/C:N/I:N/A:P (nvd)
5.0/AV:N/AC:L/Au:N/C:N/I:N/A:P (redhat)

```
Memory leak in the dtls1 buffer record function in d1 pkt.c in OpenSSL 1.0.0
before 1.0.0p and 1.0.1 before 1.0.1k allows remote attackers to cause a
denial of service (memory consumption) by sending many duplicate records for
the next epoch, leading to failure of replay detection.
```

Installed	Candidate
openssl-1.0.1e-30.el6	1.0.1e-57.el6

CVE-2015-0286
5.0 (MEDIUM) CWE-822 / CWE-125 / CWE-17
5.0/AV:N/AC:L/Au:N/C:N/I:N/A:P (nvd)
4.3/AV:N/AC:M/Au:N/C:N/I:N/A:P (redhat)

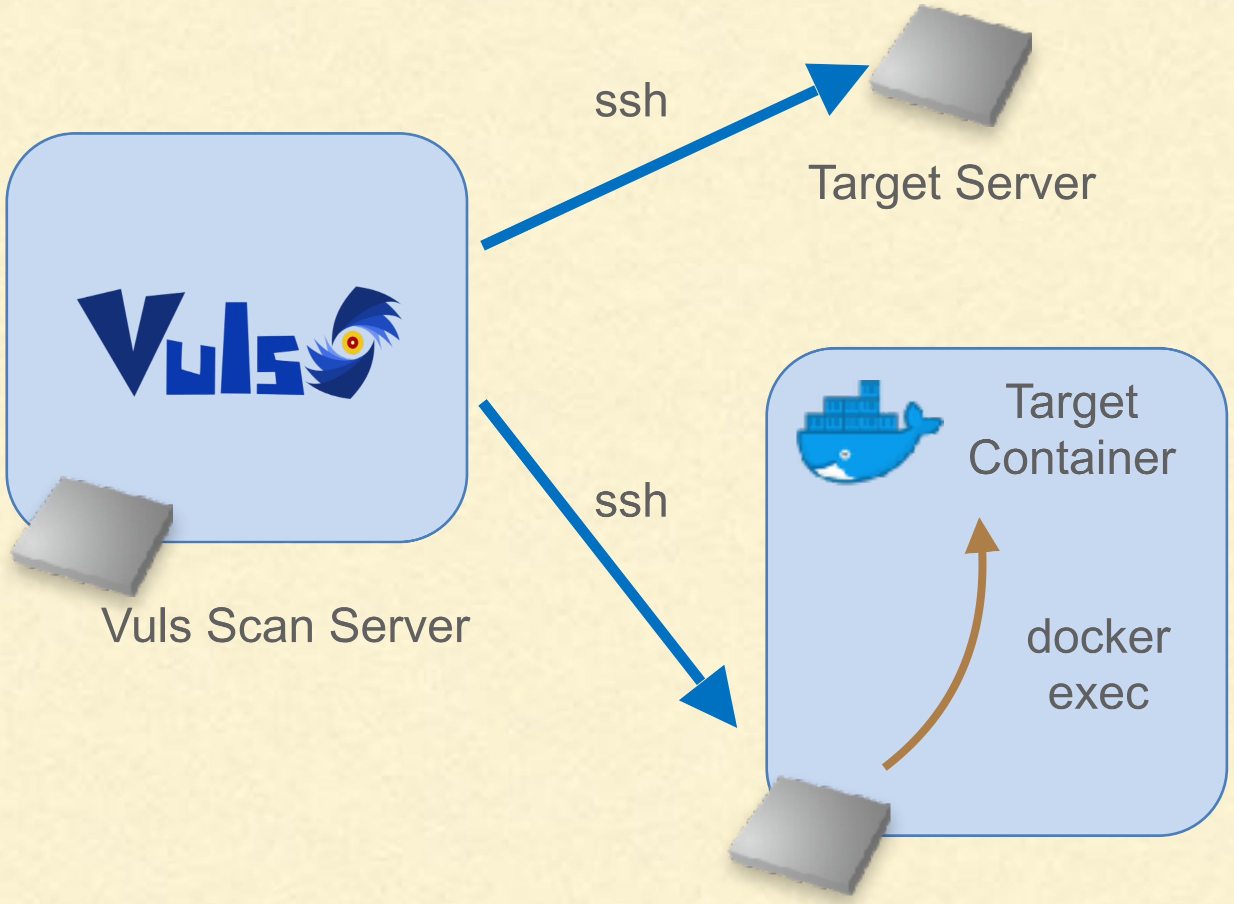
```
The ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before
0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a
does not properly perform boolean-type comparisons, which allows remote
attackers to cause a denial of service (invalid read operation and
application crash) via a crafted X.509 certificate to an endpoint that uses
the certificate-verification
```

Show more...

Installed	Candidate
openssl-1.0.1e-30.el6	1.0.1e-57.el6

Scanning Modes

Remote



ssh

Target Server

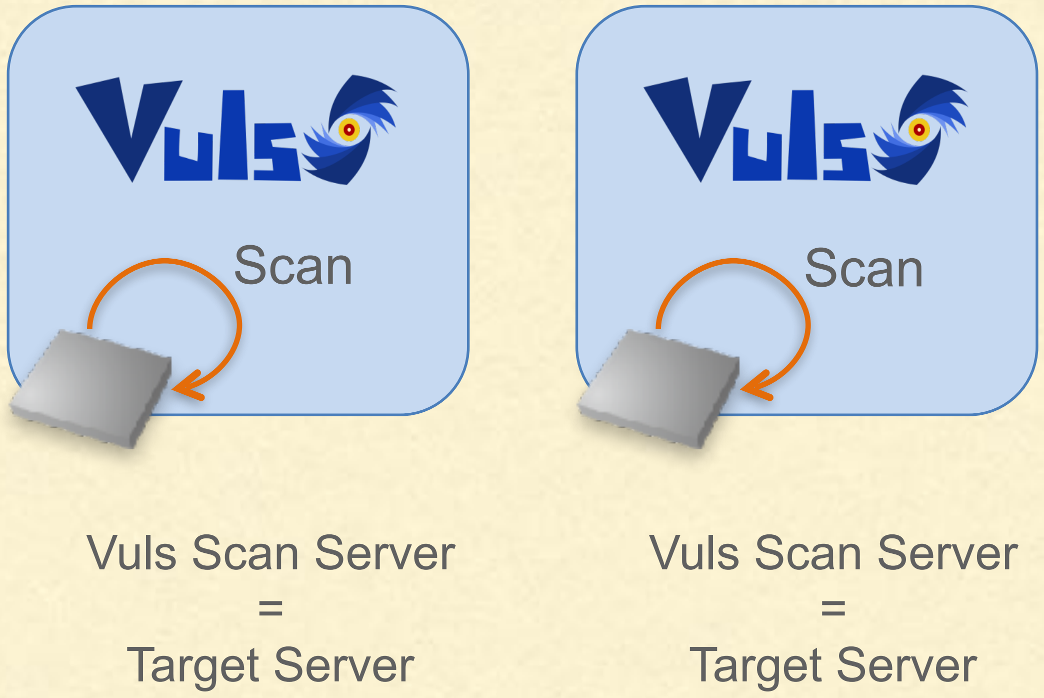
ssh

Target Container

docker exec

Vuls Scan Server

Local



Scan

Vuls Scan Server
=
Target Server

Scan

Vuls Scan Server
=
Target Server

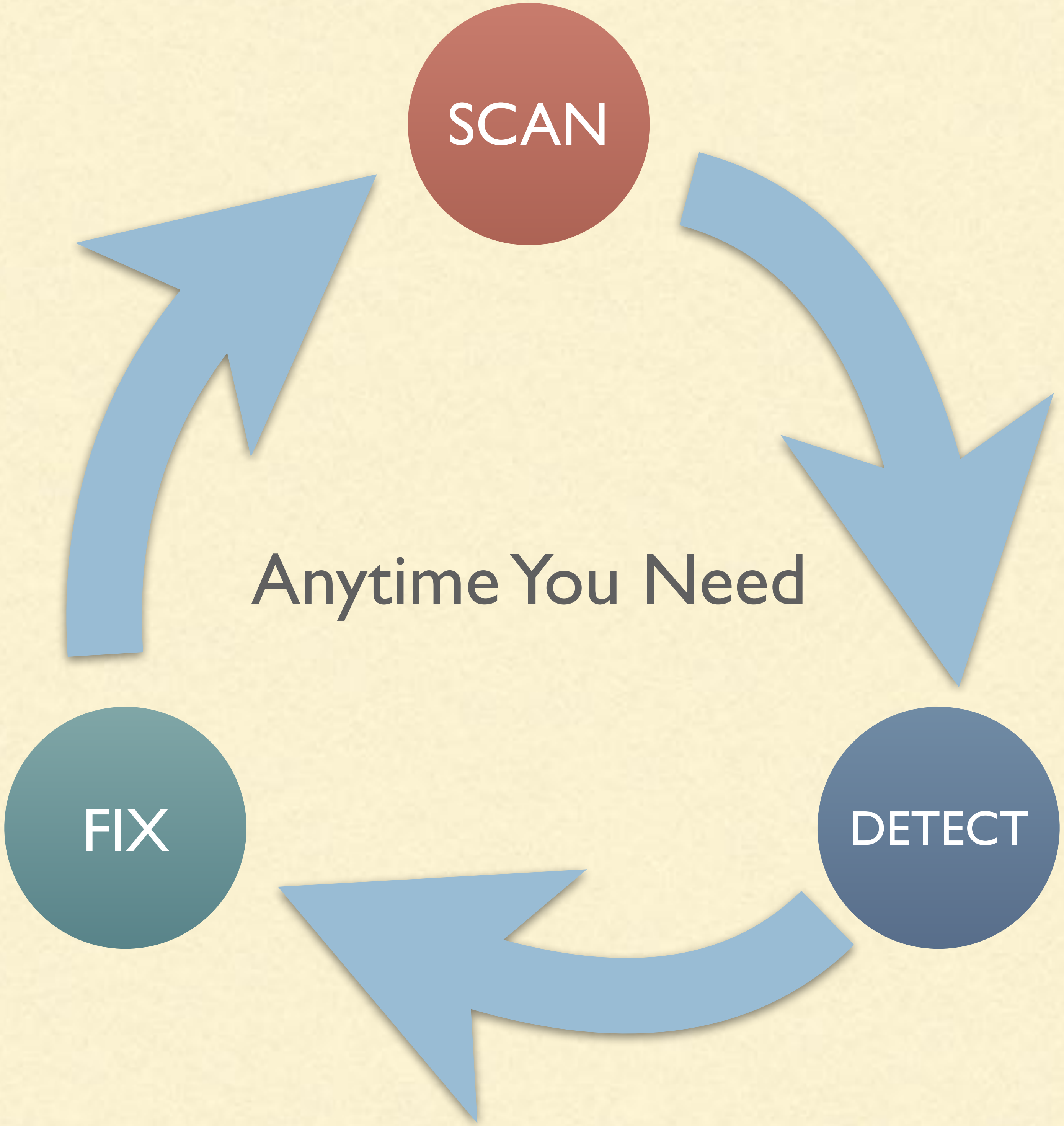
~~Penetration Testing~~?

Non-Intrusive Scans

Pre-authorization not needed when scanning on cloud

Vulnerability / Penetration Testing Request on AWS not necessary

Continuous Integration



SCAN

DETECT

FIX

Anytime You Need

circleci

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

CVE-ID

```
<title>RHSA-2017:2485: git security update (Important)</title>
<reference ref_id="CVE-2017-1000117" ... source="CVE"/>
…
<cve cvss3="6.3/CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/
A:L" href="https://access.redhat.com/security/cve/
CVE-2017-1000117" public="20170810">
cve>
...
<criterion comment="git is earlier than 0:1.7.1-9.el6_9"
test_ref="oval:com.redhat.rhsa:tst:20172485007"/>
```

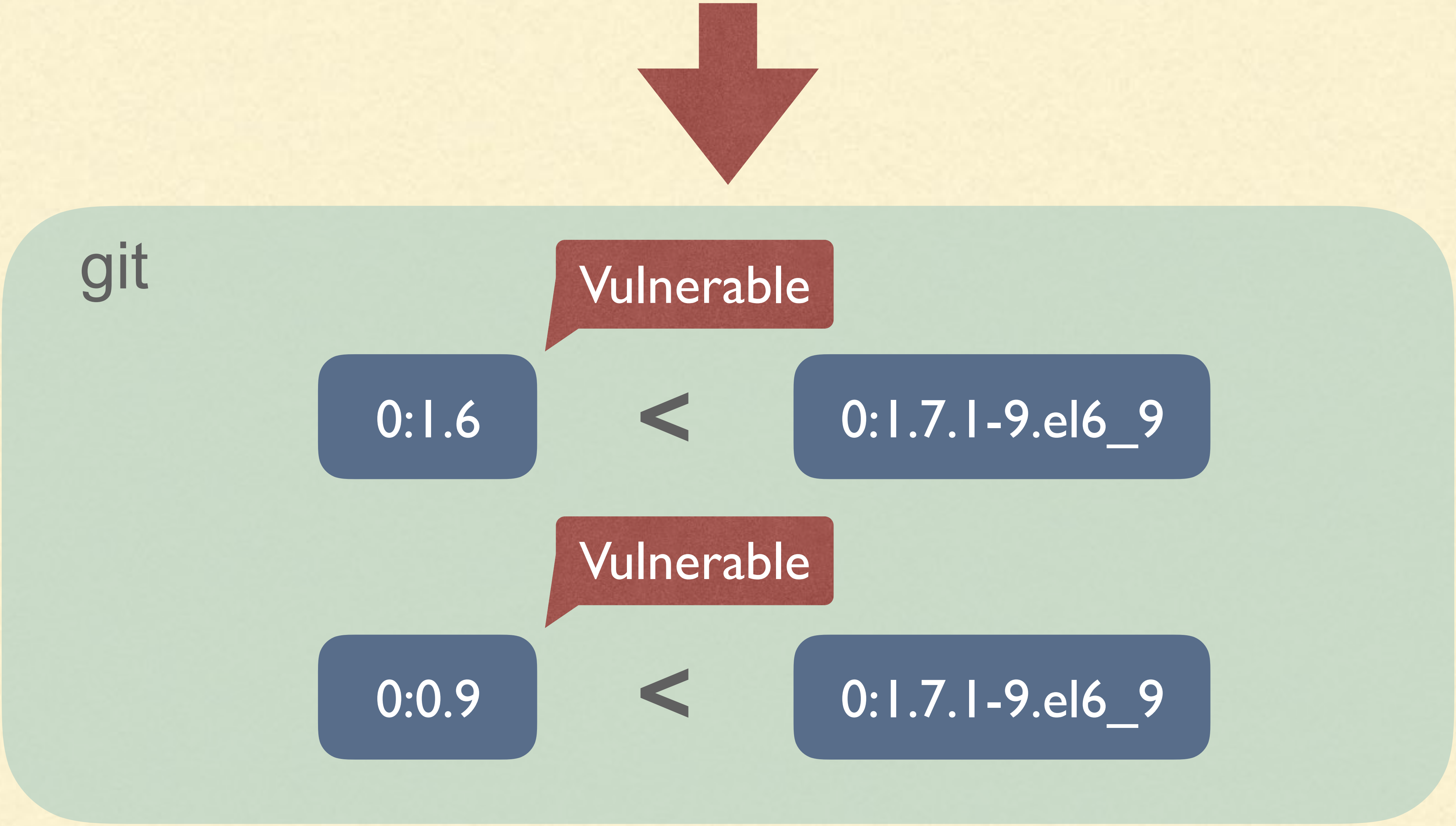
CVSS Score & Vector

Package Name

Package Version

CVE-2017-1000117

git is earlier than **0:1.7.1-9.el6_9**



git

Vulnerable

0:1.6 < 0:1.7.1-9.el6_9

Vulnerable

0:0.9 < 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
- **Red Hat**
  - **Not found**
    - Read code and guess specifications
    - https://github.com/rpm-software-management/rpm/blob/master/lib/rpmvercmp.c#L16

'1' '~' '~~' '10'

'~~a'

'a'

''

Sort versions from oldest to newest

(deb-version)

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

Old New

deb-version

?

3.6.20-1.ab1 ≶ 3.6.20-1.2

3.6.20-1.ab1 > 3.6.20-1.2

3.6.20-1.ab1 < 3.6.20-1.2

Debian

Red Hat

Compare Versions

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

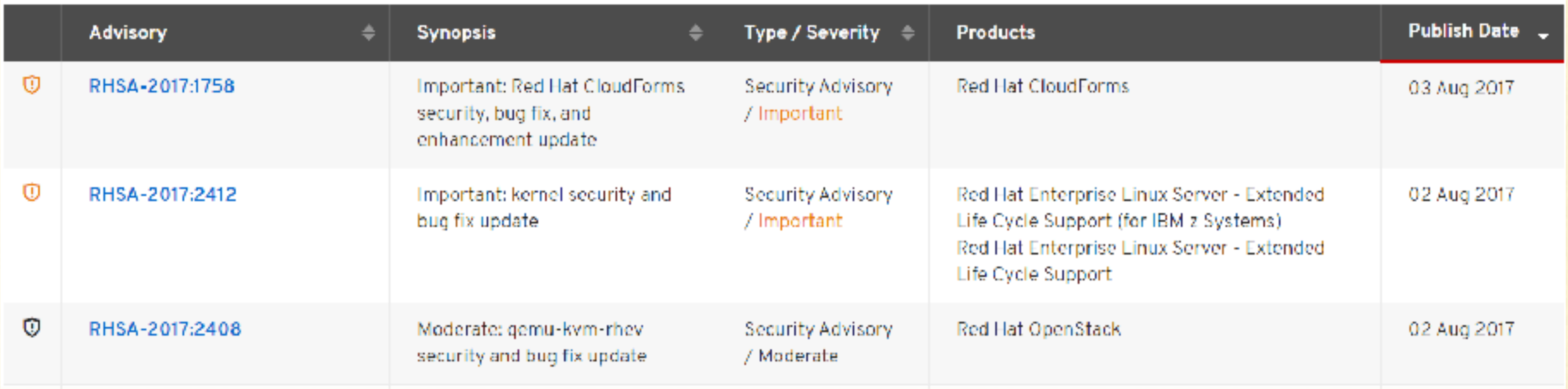
- **Debian**
  - 3.6.20-1.el6 > 3.6.20-1.2

Opposite!

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

Security Advisories

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



	Advisory	Synopsis	Type / Severity	Products	Publish Date
🛡	RHSA-2017:1758	Important: Red Hat CloudForms security, bug fix, and enhancement update	Security Advisory / Important	Red Hat CloudForms	03 Aug 2017
🛡	RHSA-2017:2412	Important: kernel security and bug fix update	Security Advisory / Important	Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) Red Hat Enterprise Linux Server - Extended Life Cycle Support	02 Aug 2017
🛡	RHSA-2017:2408	Moderate: qemu-kvm-rhev security and bug fix update	Security Advisory / Moderate	Red Hat OpenStack	02 Aug 2017

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 Advirories)

```
$ sudo yum updateinfo list
--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)

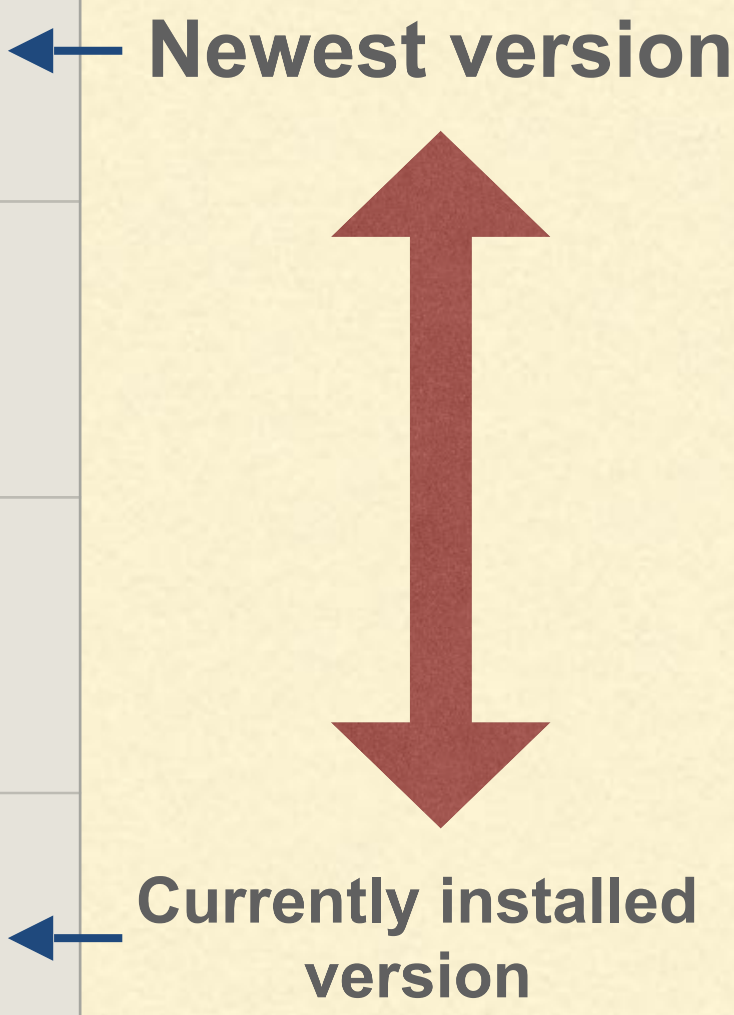
```
* Mon Dec 12 12:00:00 2016 Siteshwar Vashisht <svashisht@redhat.com> - 4.1.2-47
- CVE-2016-9401 - Fix crash when '-' is passed as second sign to popd
  Resolves: #1396383

* 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
```

Newest version

Currently installed version

Bash (Red Hat)

FIXED CVE-ID	VERSION
CVE-2016-9401	4.1.2-47
CVE-2016-7543	4.1.2-46
CVE-2016-0634	4.1.2-45
–	4.1.2-44



Newest version

Currently installed version

Unique Features

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

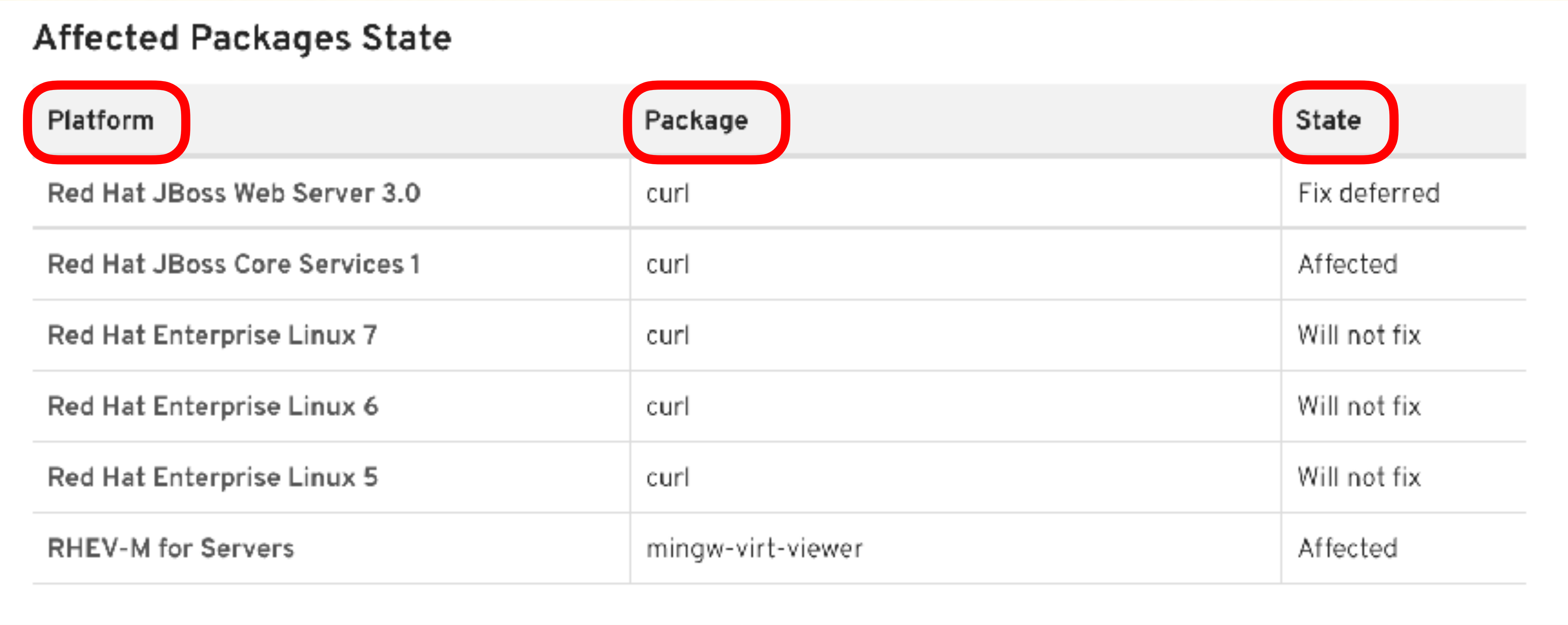
PID	Process
432	ntpd
930	**sshd**
1157	httpd

Restart required

Features In The Future

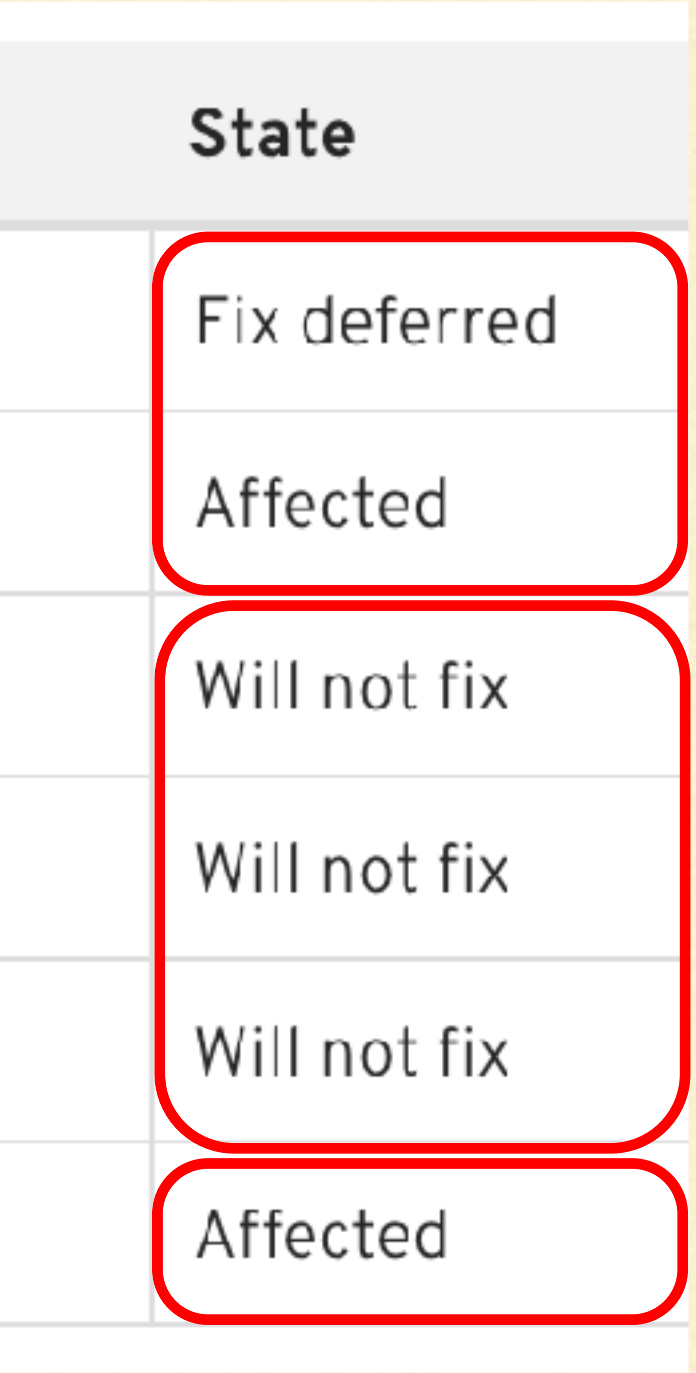
- **Detect vulnerabilities for which there’s no update yet**
  - Monitor Security Trackers (Debian, Ubuntu, Red Hat, etc)

CVE-2016-8615



Affected Packages State

Platform	Package	State
Red Hat JBoss Web Server 3.0	curl	Fix deferred
Red Hat JBoss Core Services 1	curl	Affected
Red Hat Enterprise Linux 7	curl	Will not fix
Red Hat Enterprise Linux 6	curl	Will not fix
Red Hat Enterprise Linux 5	curl	Will not fix
RHEV-M for Servers	mingw-virt-viewer	Affected



State
Fix deferred
Affected
Will not fix
Will not fix
Will not fix
Affected

No update yet

Will not fix

No update yet

Features In The Future

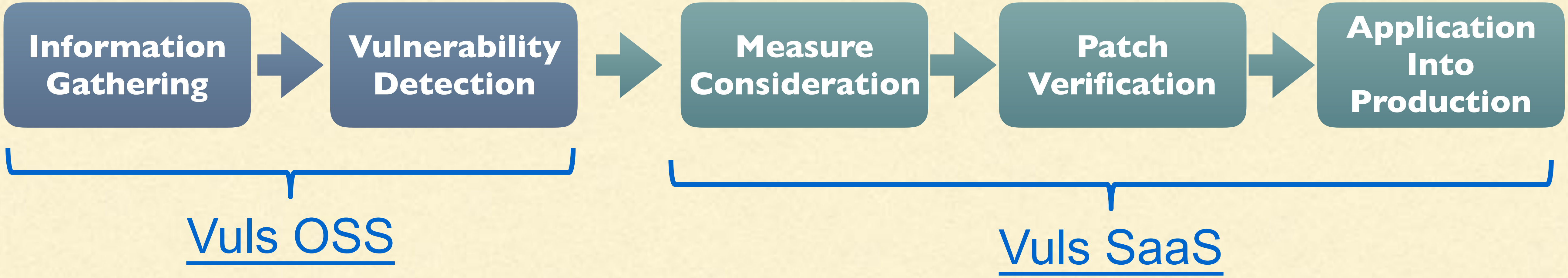
- **Find Exploit Code (PoC)**
  - The Exploit Database, Metasploit, etc.

EXPLOIT DATABASE

metasploit®

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

On-Premise and Cloud

Fast

High-quality

Flexible

Extensive OS Support

Thank you for your time!

kotakanbe@gmail.com
knqyf263@gmail.com