Praca inżynierska

System raportowania informacji o znanych podatnościach

Patryk Gałczyński
Promotor: dr inż. Marek Zachara

AKADEMIA GÓRNICZO-HUTNICZA IM. STANISŁAWA STASZICA W KRAKOWIE
AGH UNIVERSITY OF SCIENCE AND TECHNOLOGY

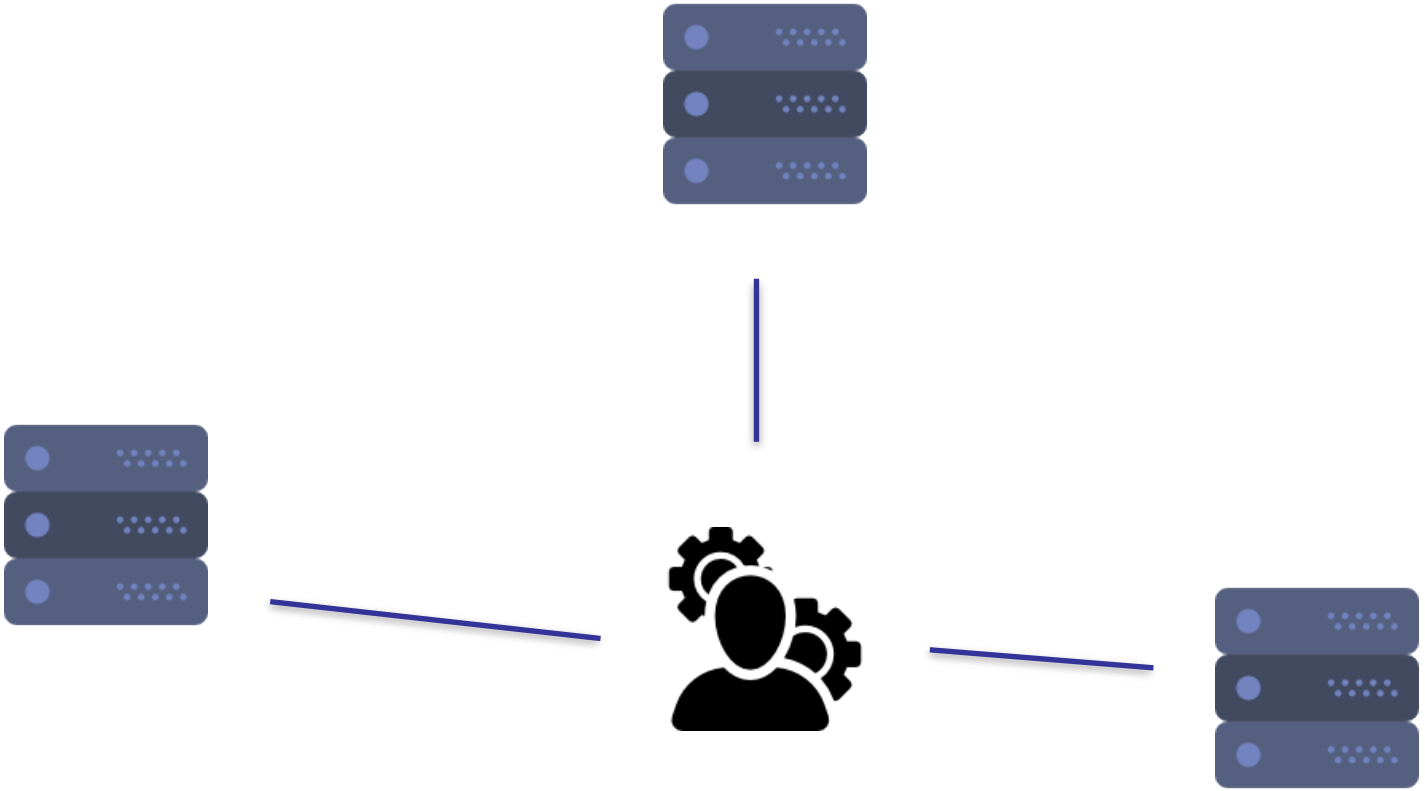
21.11.2017

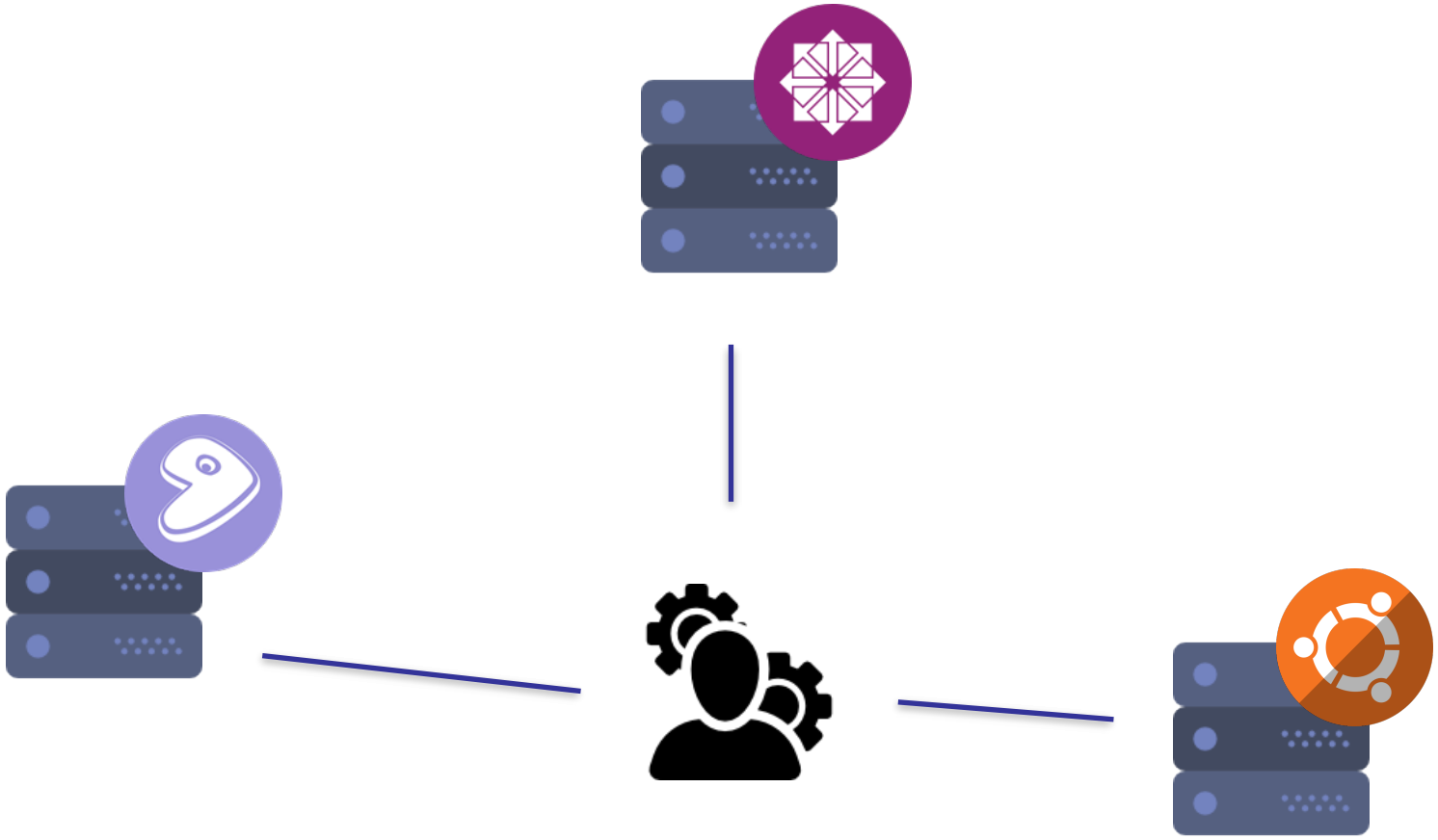
Agenda

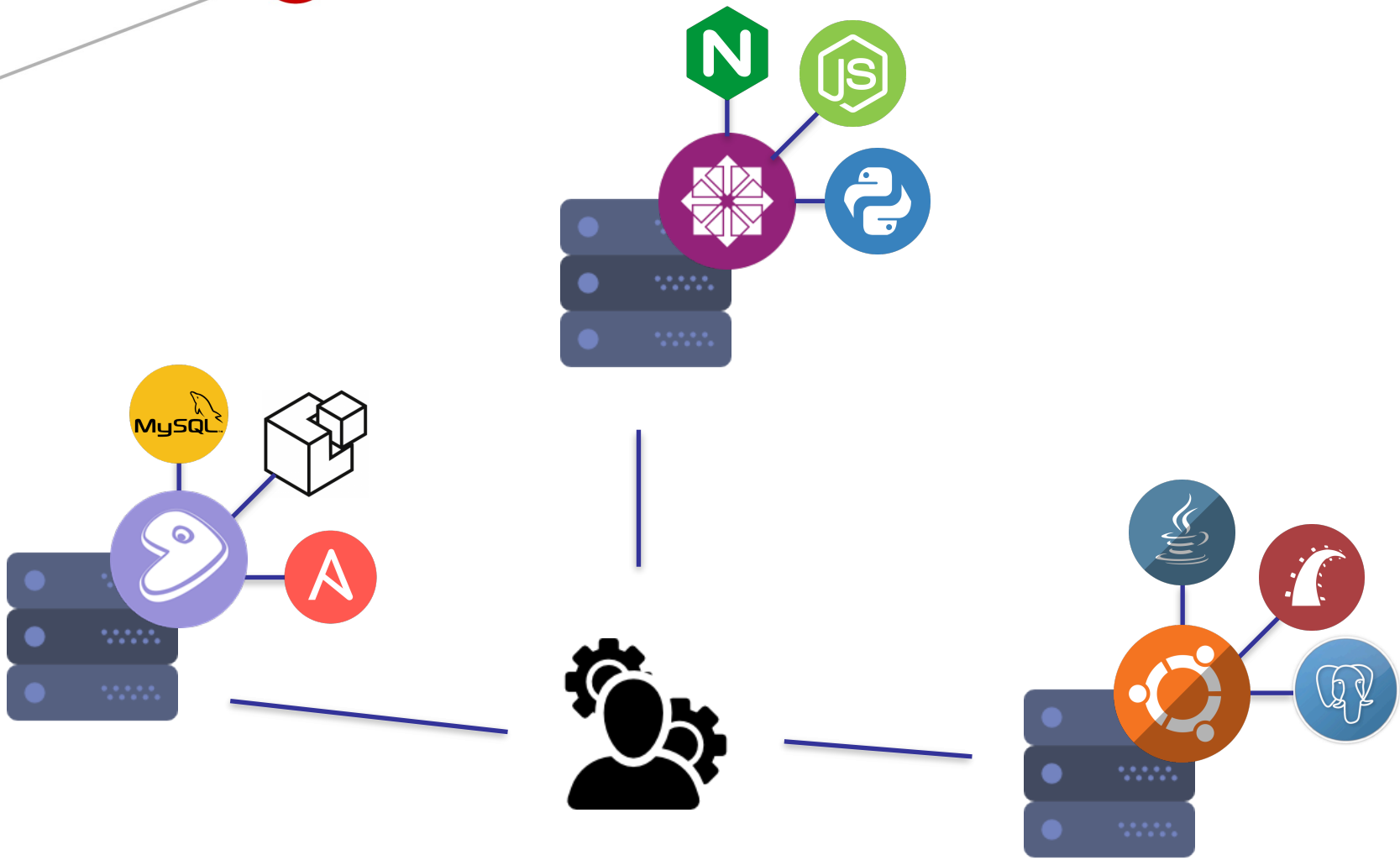
1. Wstęp
2. Agenda
3. Cele pracy
4. Architektura i pojęcia
5. Wnioski
6. Podsumowanie i wnioski
7. Pytania?
8. Zakończenie

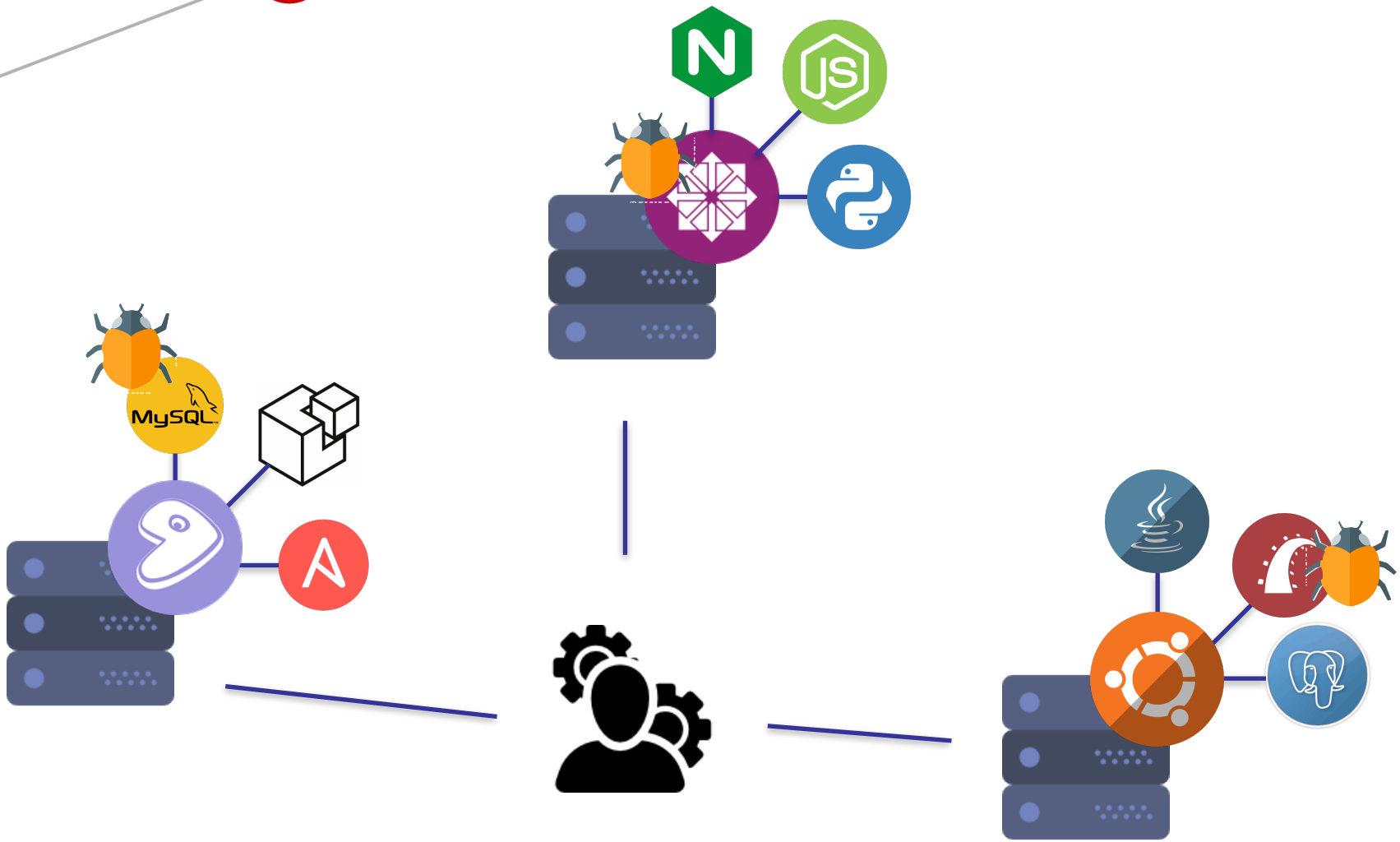
Cele pracy

Aplikacja wspomagająca pracę administratora w zakresie **identyfikacji oraz powiadamiania** o znanych **podatnościach** utrzymywanych systemów






MySQL


MySQL

Cele pracy

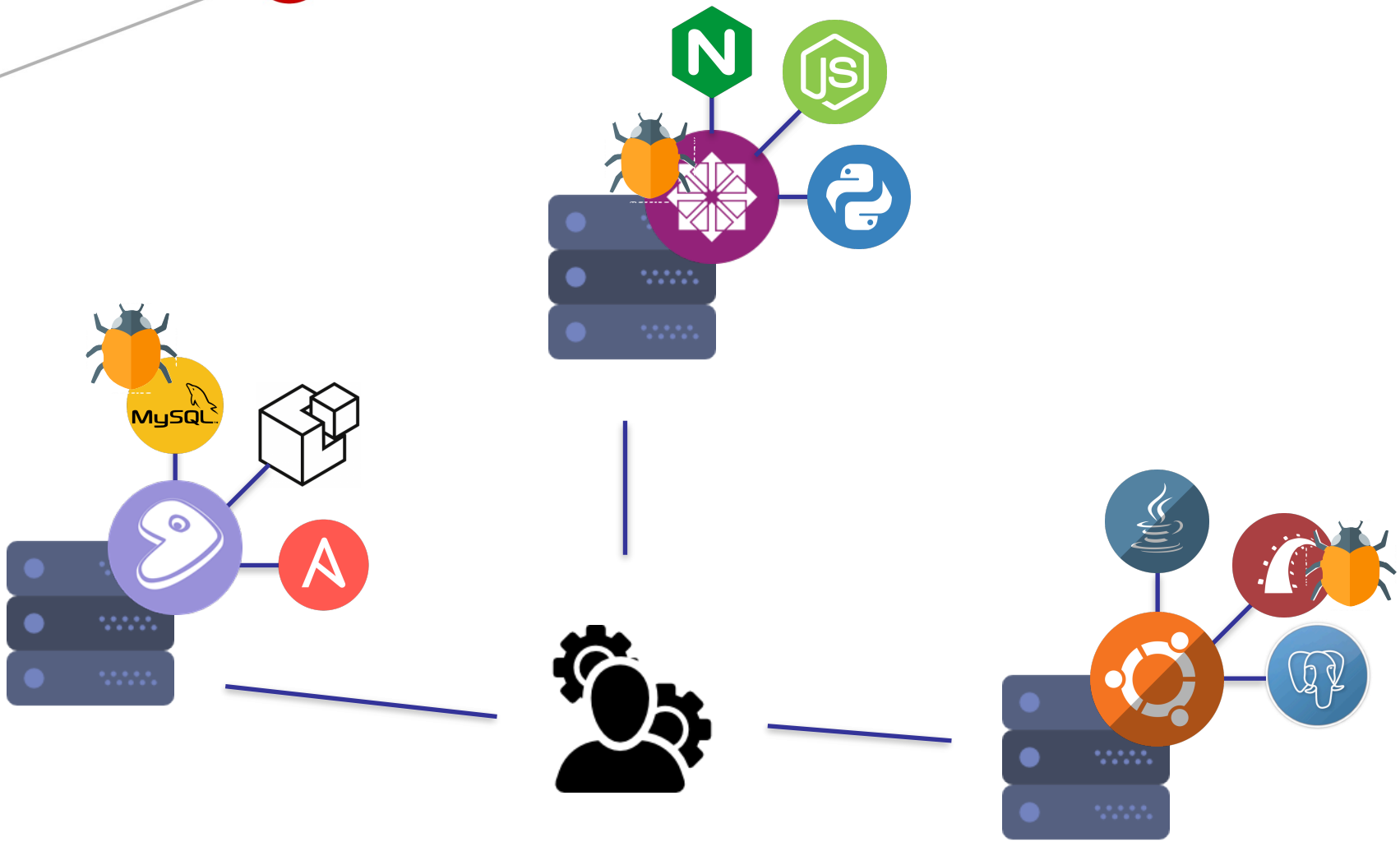
Aplikacja wspomagająca pracę administratora w zakresie **identyfikacji oraz powiadamiania** o znanych **podatnościach** utrzymywanych systemów

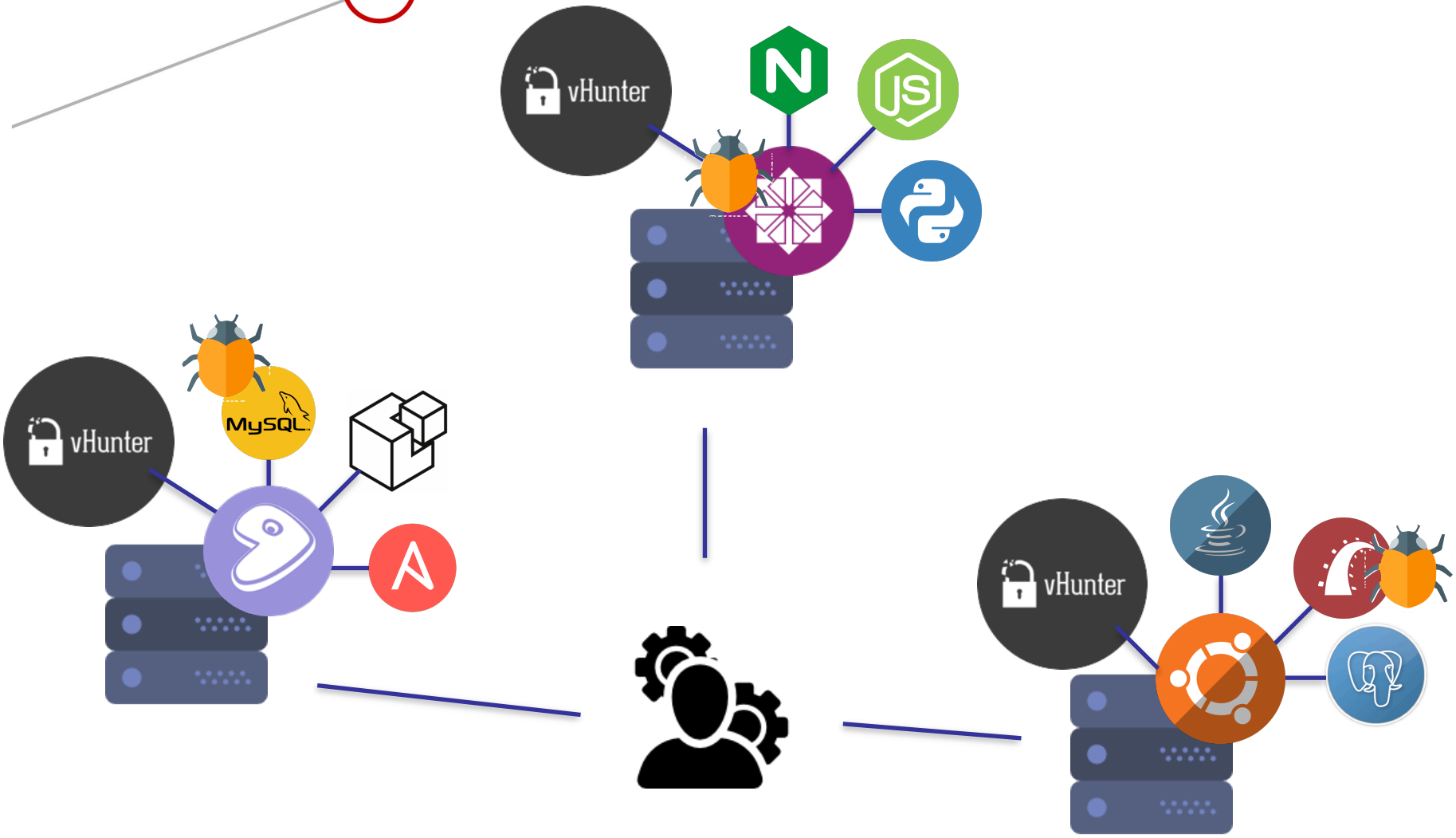
Cele pracy

Aplikacja wspomagająca pracę administratora w zakresie **identyfikacji oraz powiadamiania** o znanych **podatnościach** utrzymywanych systemów

1. Nie zależna od platformy i dystrybucji
2. Łatwo rozszerzalna i konfigurowalna
3. Obsługująca zarówno:
    1. Pojedyńcze maszyny
    2. Całe klastry maszyn
4. Umiejąca powiadamiać o znalezionych podatnościach

AGH


MySQL


vHunter
vHunter
MySQL
vHunter

Architektura

Python
- nie zależny od platformy
- działa prawie na wszystkim
- posiada rozwiniętą społeczność

Yaml
- czytelny dla człowieka
- elastyczny format serializacji
- duże możliwości
- przekłada się bezpośrednio
  na struktury danych
  w językach programowania

Pojęcia

Scenariusz - ciąg poleceń definiujących określone zachowanie dla danej platformy

```
2 c/s/list-apps.yaml  2 c/s/list-python-packages.yaml
" Press ? for help                 | 1 list-apps-scenario:
                                   | 2     job:
.. (up a dir)                      | 3         ubuntu: dpkg -l | awk ''{ print $2 \",\" $3}'' | tail -n +6
</studia/vHunter/vHunter/          | 4         centos: yum list
▾ conf/                            | 5         osx: brew list --versions | sed -e ''s/ /,/g''
  ▾ scenarios/                     | 6         default: echo ''distro not found''
      list-apps.yaml               | 7
      list-python-packages.yaml    |~
```

```
12:38:36 evemorgen@Patryks-MacBook-Pro.local ~ brew list --versions | sed -e 's/ /,/g'
aria2,1.33.0
autoconf,2.69
cmake,3.9.5
curl,7.56.0
ffmpeg,3.4
gdbm,1.13
```

Pojęcia

Baza podatności - słownik identyfikatorów odpowiadających powszechnie znanym podatnościom oraz zagrożeniom, a także standard ich nazewnictwa

Głównie używane bazy

1. CVE (Common Vulnerabilities and Exposures)
2. NVD (National Vulnerability Database)
3. Dowolna inna zdefiniowana w *vHuner/db_drivers*

Pojęcia

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2016-10096 Detail

Current Description

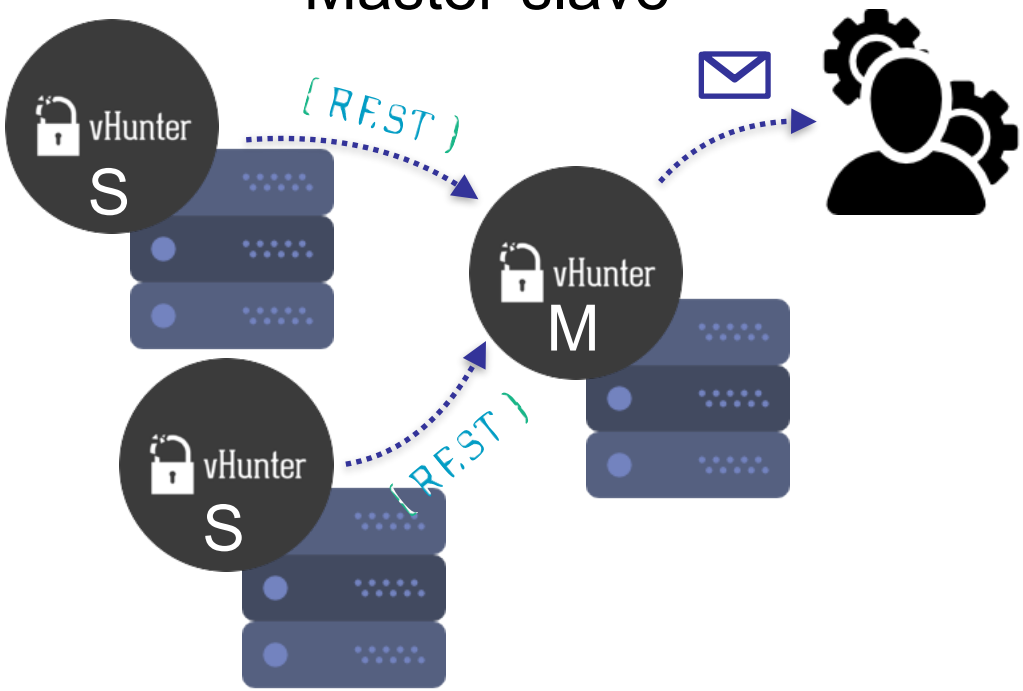
SQL injection vulnerability in register.php in GeniXCMS before 1.0.0 allows remote attackers to execute arbitrary SQL commands via the activation parameter.

Source: MITRE **Last Modified:** 01/01/2017 View Analysis Description

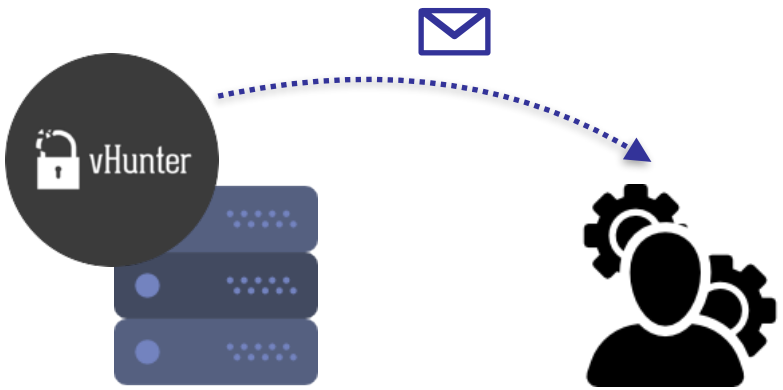
Pojęcia

Tryb **master-slave** oraz **master-less** - tryby działania aplikacji vHunter

Master-slave



Master-less



Pojęcia

CLI (*Command Line Interface*) - interfejs wiersza poleceń

Zapewnia dostęp do łatwej konfiguracji narzędzia w przyjaznej formie dla administratora

```
(ENV) 13:26:06 evemorgen@Patryks-MacBook-Pro.local vHunter feature/basic_setup ? python main.py -h
usage: main.py [-h] [-a] [-ms] [-m] [-s] [-S SCENARIO] [-c CONFIG]
               [-l LOG_FILE] [-L LOG_LEVEL] [-p PORT] [-H HOST] [--list]

vHunter is a automated reporting and searching system for known system
vulnerabilities

optional arguments:
  -h, --help            show this help message and exit
  -a, --stand-alone     vHunter will operate in standalone more, means it
                        won't try to form clusters
  -ms, --master-slave   vHunter will try to form cluster, due to avoidance of
                        spamming sysadmins
  -m, --master          Node will act as a master.
  -s, --slave           Node will act as a slave. vHunter-slave will try to
                        connect to master on defined port (default is 1911)
  -S SCENARIO, --scenario SCENARIO
                        path to directory keeping scenarios to check
  -c CONFIG, --config CONFIG
                        path to config user config file, default is
                        /etc/vHunter.yaml
  -l LOG_FILE, --log-file LOG_FILE
```

Wnioski

W ramach pracy inżynierskiej powstało **otwarte** i darmowe narzędzie **wyszukujące podatności** w systemie oraz **powiadamiające** administratora. Jest ono bardzo **łatwo rozszerzalne** o kolejne moduły.

Cel pracy został zrealizowany.

Pytania?

Zakończenie

Dziękuję za uwagę