

Безопасность инфраструктуры

Не забудь включить запись!



План

- Возможные типы атак
- Сравнения облаков с точки зрения безопасности
- Разбор инструментария

Немного статистики

70% атак стали возможны благодаря нарушению элементарных правил безопасности

По данным USA Cert, OWASP Security Research

Причины

- Firewall - для слабых духом
- Доступ в инфраструктуру через DST NAT (VPN для слабых духом)
- Постоянная работа от root`а
- Отсутствие разделения в окружениях

Многовекторные атаки

- Script kiddy (мамкин хакир)
- Профессиональные группировки (Anonymous, LulzSec, Шалтай-болтай)
- - Атаки исключительно на фин. тех (Cobalt, Silence) (Привет ребятам из Индии)

Софт и железо

Аппаратные vs. Программные

Аппаратные:

- Spectre
- Meltdown

Программные

- 0-day
- И тд. и тп.

Другие возможности

Не стоит забывать и про людей

Люди и twitter



We are giving back to our community. We support Bitcoin and we believe you should too!

All Bitcoin sent to our address below will be sent back to you doubled!

Облачные провайдеры

GCP vs. Ya.cloud

Облачные провайдеры

GCP

- Облачный Firewall
- Гибкая настройка сети
- Гибкая настройка прав в проектах

Ya.cloud

- Настройка выделенной сети

Облачные провайдеры

GCP

- Часть вопросов безопасности мы можем вынести на сторону платформы

Ya.cloud

- Много придется делать на инстансах

Операционные системы

- SELinux
- AppArmor
- PolicyKit
- ACL
- chroot/namespaces/cgroups
- iptables/firewalld

Инструментарий

- Terraform
- Ansible
- AWS Cloudformation
- Все что работает через API с провайдером

Terraform

```
provider "yandex" {  
  token      = "111122222333333"  
  cloud_id   = "111122222333333"  
  folder_id  = "111122222333333"  
  zone       = "ru-central1-a"  
}
```

22% конфигураций содержат "чувствительные" данные

Terraform

66% of cloud user-configured S3 buckets do not have logging enabled

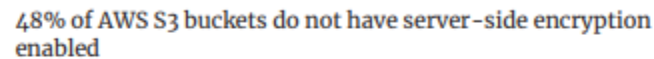
26% of cloud user-configured AWS EC2 instances have SSH (port 22) exposed to the internet

17% of cloud user-configured AWS Security Groups allow ALL inbound traffic (0.0.0.0/0)

AWS Cloudformation

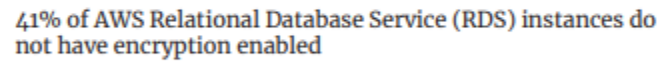
```
"S3Bucket": {  
  "Type": "AWS::S3::Bucket",  
  "Properties": {  
    "AccessControl": "PublicRead",  
    "BucketName": "${project}-${stage}"  
  }  
}
```

AWS Cloudformation



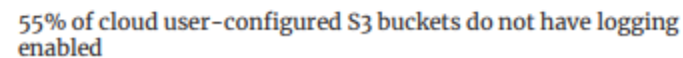
48% of AWS S3 buckets do not have server-side encryption enabled

A horizontal bar chart with a blue bar representing 48% of the total. The bar is followed by a dotted line extending to the right.



41% of AWS Relational Database Service (RDS) instances do not have encryption enabled

A horizontal bar chart with a blue bar representing 41% of the total. The bar is followed by a dotted line extending to the right.



55% of cloud user-configured S3 buckets do not have logging enabled

A horizontal bar chart with a blue bar representing 55% of the total. The bar is followed by a dotted line extending to the right.

Ansible

- Чувствительные данные в переменных
- Ssh ключи
- Бесконечный become

Общая конфигурация

Afraid 777

Инструментарий в ПОМОЩЬ

- Wazuh
- Zabbix + security plugins
- OSSIM
- Etc.