{AB}USE their Clouds

Облачные вычисления глазами пентестера

Сергей Гордейчик
Юрий Гольцев
Positive Technologies

Что такое «Облачные вычисления»?

- SaaS (Software as a service)
- PaaS (Platform as a service)
- IaaS (Infrastructure as a service)
- HaaS (Hardware as a Service)
- WaaS (Workplace as a Service)
- IaaS (Infrastructure as a service)
- EaaS (Everything as a Service)
- DaaS (Data as a Service)
- SaaS (Security as a Service)

Что в облаке тебе моем

- Анонимность и сокрытие следов
- Экономическая эффективность
- Сканирование портов
- «Роботизация» сбора информации
- Подбор паролей
- «Нагрузочное тестирование»
- Кое-что еще…
- Атаки на облако

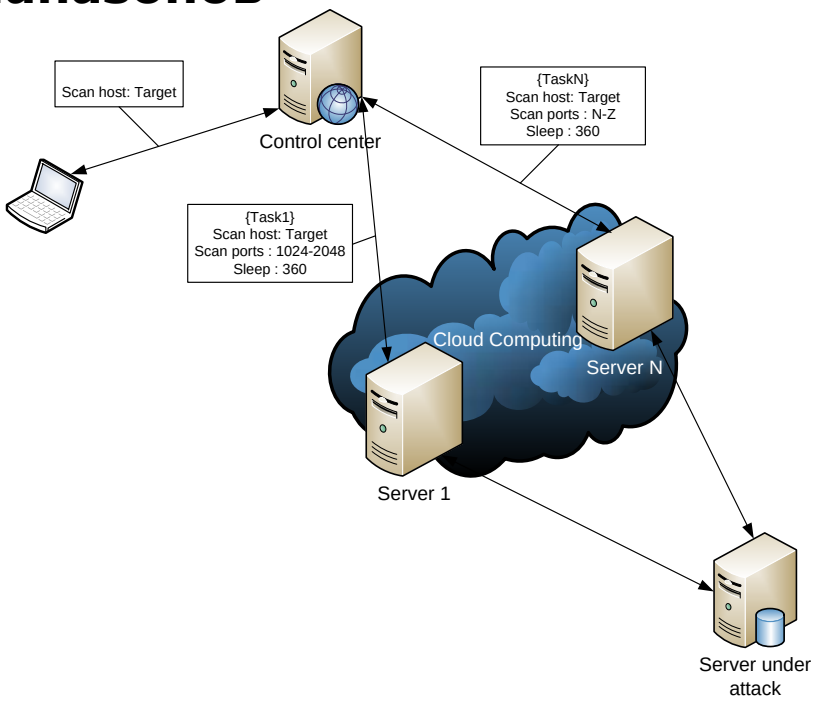
Анонимность и сокрытие следов

- **По степени верификации большинство IaaS-сервисов сопоставимо с ISP: платежная информация, сотовый телефон (опционально)**

- **Наличие тестового доступа (email, IP-адрес)**
- **В ряде ситуаций instance уничтожается после использования**

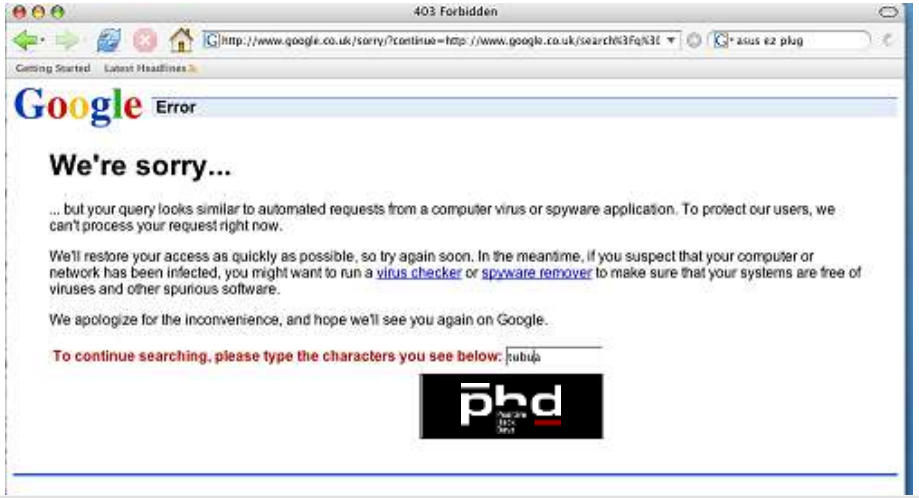
Сканирование портов

- **Использования большого количества IP-адресов и узлов**
- **Сканирование масштабных диапазонов**
- **«Долгие» задачи (UDP)**
- **Обход IPS (задержки)**
- **Практическая реализация:**
  - **Nmap/unicorscan**
  - **немного PHP**



«Роботизация» сбора информации

- **Googlehack, подбор адресов email, индексация сайтов, перебор «секретных» ссылок**
- **Аналогично сканированию портов**
  - Использования большого количества IP-адресов и узлов
  - Сканирование масштабных диапазонов
  - Обход IPS и защитных механизмов
- **Практическая реализация:**
  - Ваш любимый toolkit
  - немного PHP

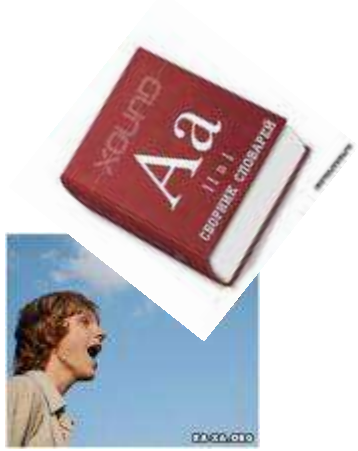


Подбор паролей

- Online bruteforce
- Генерация и хранение Rainbow Tables
- Offline bruteforce

Online bruteforce

- **Обход ограничений попыток на IP/сессию**
  - Microsoft RDP
  - Cisco
- **Подбор в больших сетях**
  - 1000 рутеров
  - Возможно одинаковый пароль
  - По одному паролю на каждой



Атака со словарем

Rainbow tables

ntlm (mixalpha-numeric-all-space,8)

Ресурс	Количество	Стоимость	Общая стоимость
Instance	20	$6590 + $0,56/hour	20 * $6590 = $131 800 $ 0,56 * 20 * 12834 = $ 143 740
Data Storage	418 Tb	$ 102 / Tb	$ 102 * 418 =$ 42 636
Итого			$ 318 176

2 x Intel Xeon X5570 4Core “Nehalem” X 20 = 18 месяцев + $320 000

Desktop = 1290 лет

Rainbow tables

Rainbow	Время	$
Цифры (от 1 до 12 символов)	3 часа	103 $
Символы английского (low-case) алфавита (от 1 до 12 символов)	21 год	$2 363 252
Символы английского алфавита (от 1 до 11 символов)	275 суток	$ 754 064
Символы английского алфавита (low-case) (от 1 до 10 символов)	11 суток	$ 9 823
Символы английского алфавита (low-case) и цифры (от 1 до 12 символов)	1046 лет	$80 919 507
Символы английского алфавита (low-case) и цифры (от 1 до 11 символов)	27 лет	$ 4 631 216
Символы английского алфавита (low-case) и цифры (от 1 до 10 символов)	297 суток	$ 188 884
Символы английского алфавита (low-case) и цифры (от 1 до 9 символов)	11 суток	$ 9 695

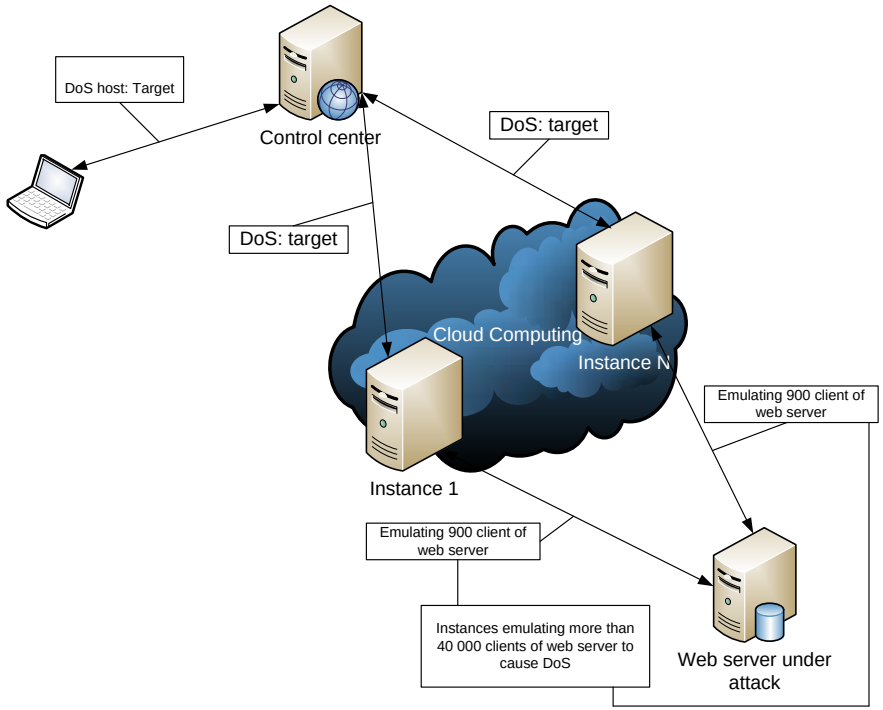
Offline bruteforce

Сплошное удовольствие!

En-low-case-digit-11	MD4	~ 10 лет	$ 183 960
	MD5	~ 9 лет	$ 165 564
	SHA1	~ 16 лет	$ 294 336
	NTLM	~ 11 лет	$ 202 365
En-low-case-digit-10	MD4	~ 108 дней	$ 5 443
	MD5	~ 92 дней	$ 4 636
	SHA1	~ 165 дней	$ 8 316
	NTLM	~ 111 дней	$ 5 594
En-low-case-digit-9	MD4	~ 72 часа	$ 151
	MD5	~ 61 часа	$ 128
	SHA1	~ 110 часов	$ 231
	NTLM	~ 74 часа	$ 155

«Нагрузочное тестирование»

- **Средней силы DoS (200 000 активных соединений)**
- **SlowPost.pl**
- **3 сотовых SIM (900 руб)**
- **46 Instance на 2 часа (240 руб)**
- **Трафик (8 рублей)**

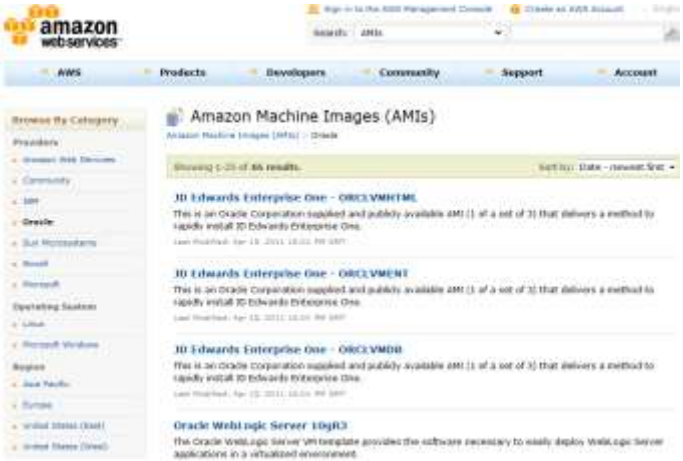


- **Итого: 1150 руб**

Кое что…

- **Пользователи могут сохранять Amazon Machine Images (AMIs)!**
- **Пользователи могут публиковать свои AMIs!**
- **Пользователи могут использовать чужие AMIs!**

WOW!!!!



- **Linux + удобный набор софта**
- **Соглашение о сборе статистики**
- **HTTP GET при старте**
- **Более 1000 «отстуков» за месяц**

Abuse report

- **Большинство провайдеров имеют политику обработки abuse**

- **…Complaints of rampant SIP Brute Force Attacks coming from servers with Amazon EC2 IP Addresses cause many admins to simply drop all Amazon EC2 traffic….**
- **…I submitted a report to Amazon complaining of the attack…**
- **…Kay did not answer any of the additional questions we asked, but did state that she'd be interested in hearing about the other cases….**

Атаки на облако

HINT

13:00 DNS Rebinding возвращается

Денис Баранов, Positive Technologies

Links

- http://www.ptsecurity.ru/download/PT-Metrics-Passwords-2009.pdf
- http://stacksmashing.net/2010/11/15/cracking-in-the-cloud-amazons-new-ec2-gpu-instances/
- http://hashcat.net/oclhashcat/
- http://ha.ckers.org/blog/20090617/slowloris-http-dos/
- http://www.defcon.org/images/defcon-18/dc-18-presentations/Bryan-Anderson/DEFCON-18-Bryan-Anderson-Cloud-Computing.pdf
- http://www.voiptechchat.com/voip/457/amazon-ec2-sip-brute-force-attacks-on-rise/

{AB}USE their Clouds

Сергей Гордейчик
Юрий Гольцев
Positive Technologies