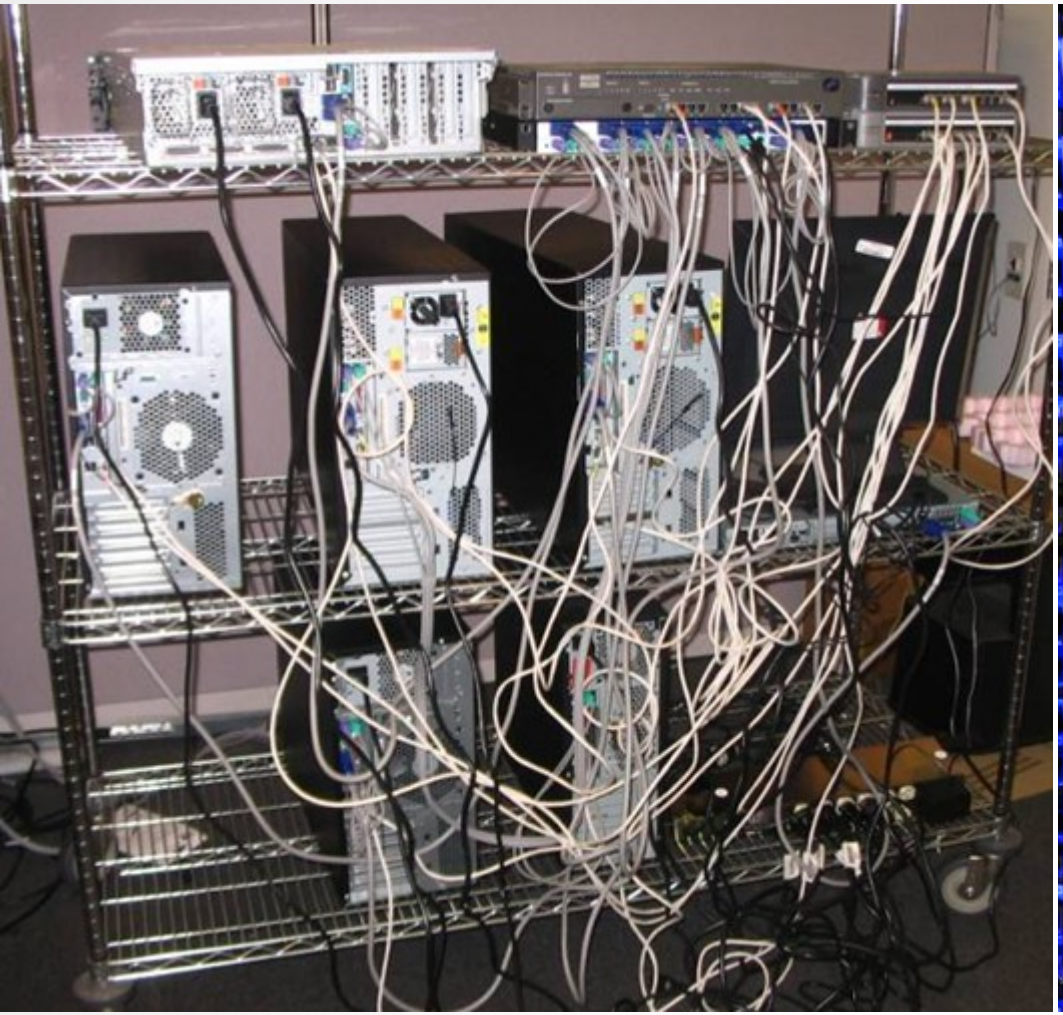
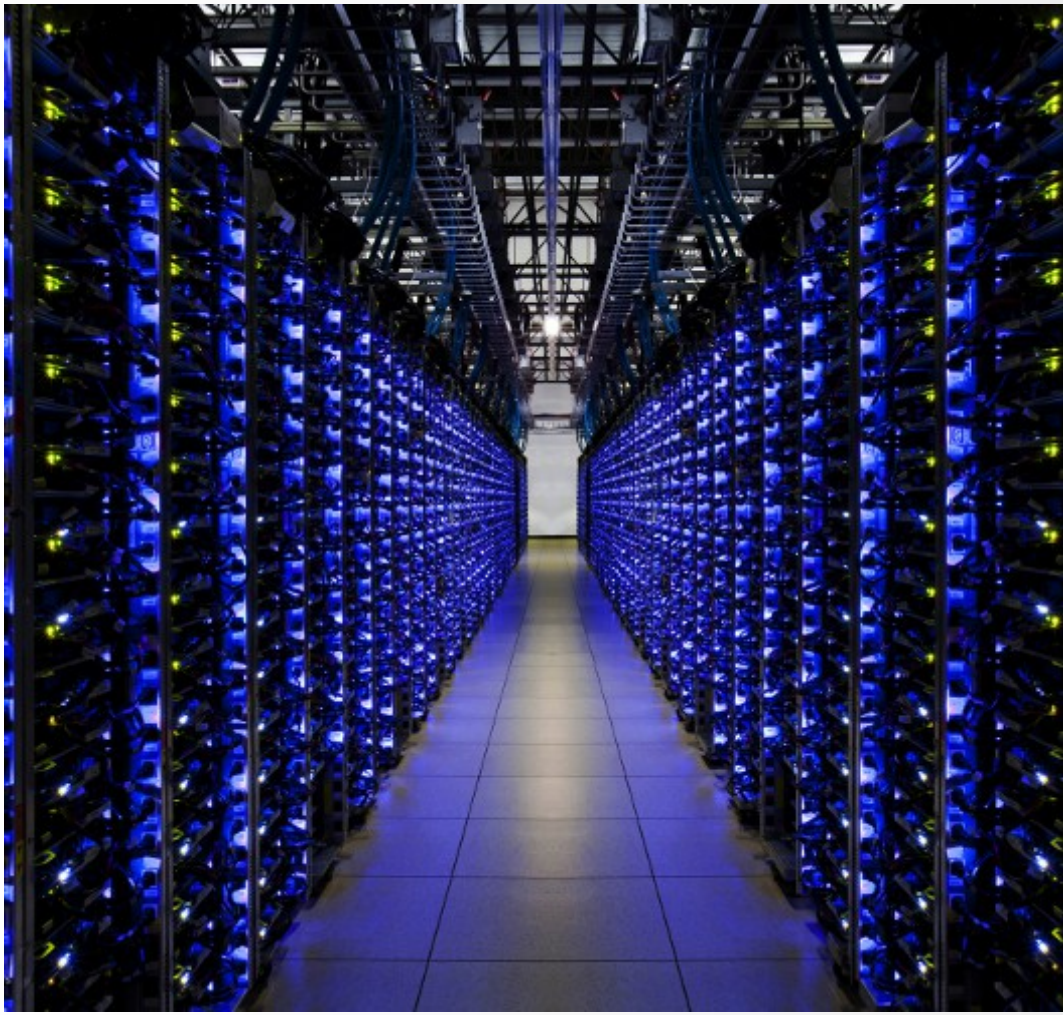
RAISIN/CEPAGE : séminaire web

Aurélien Dumez – Inria

Infrastructure et paysage

Pourquoi ?





Définir l'architecture (1/3)

Questions initiales

- **Combien de sites ? Quels types ?**
  - Applications web, CMS (WordPress, Joomla!...)
  - Langages : PHP, Java, Python, Ruby...
  - Bases de données : historiquement de type SQL mais de plus en plus souvent noSQL
- **Quelle volumétrie initiale/prévisible ?**
  - Stockage : local, NFS, GlusterFS... système de sauvegarde à ne pas négliger
  - Trafic HTTP : selon le type de site (intranet, conférence, page utilisateur...)

Définir l'architecture (2/3)

Questions initiales

- **Quelle disponibilité ?**
  - Réactivité des sites : impact d'une charge système importante générée par un site sur les autres
  - Mises à jour système avec reboot : impact d'une indisponibilité de quelques minutes
- **Accès utilisateur**
  - Approvisionnement : automatique, par demande de support
  - Gestion des données : accès aux fichiers HTML, PHP, aux bases de données (interface d'admin)
  - Statistiques et logs : indicateurs, périodicité

Définir l'architecture (3/3)

Quelques modèles

- **Hébergement classique**
  - Hébergement physique privé (1 site par serveur physique)
  - Hébergement virtuel privé (1 site sur un serveur virtuel)
  - Mutualisé (plusieurs sites sur un même serveur, virtuel ou non)
- **Hébergement nébuleux**
  - Conteneurs applicatifs (exemple : 1 CMS par conteneur)

Offre logicielle (1/2)

Environnement GNU/Linux

- **Système d'exploitation**
  - RedHat EL, EV, CentOS
- **Virtualisation**
  - Xen, VMWare, LXC, Docker
- **Gestion de configuration**
  - CFEngine, Puppet, Ansible
- **Haute disponibilité et équilibrage de charge**
  - Heartbeat, Keepalived, Pound

Offre logicielle (2/2)

- **Serveurs web**
  - Apache httpd, Nginx, Lighttpd, IIS
- **Exécution de scripts**
  - PHP : mod_PHP, php-fpm
  - Python : flup, uwsgi
  - Ruby : phusion passenger, rack
- **Systèmes de gestion de bases de données**
  - SQL : PostgreSQL, MySQL/MariaDB
  - NoSQL : MongoDB, Redis

Déployer la plateforme (1/2)

- Serveurs en DMZ
  - Protéger les réseaux internes et les serveurs entre eux
  - Au besoin, de multiples DMZ isolées (sites institutionnels, sites expérimentaux)
- Installation minimale
  - Rôle unique par serveur
  - pas d'outils de développement
- Contrôle des fichiers de configuration par défaut
  - Limiter l'émission d'informations utiles aux pirates (`ServerTokens` et `ServerSignature` sur httpd)

Déployer la plateforme (2/2)

- Serveur web : simple utilisateur
  - Jamais root
  - Utilisateur sans shell défini, ni mot de passe/clé SSH
  - Pas plus de privilèges que nécessaire
- Centralisation des données
  - Fichiers web, bases de données, journaux système
  - Décharger les serveurs et fiabiliser le stockage
- Surveillance
  - Obligatoire

Sécuriser la plateforme (1/5)

- Sécurité : ~~Produit~~ Processus
- Présent à chaque étape du déploiement
- Difficile à réaliser a posteriori
- Protéger et se protéger du code «maison»

```
<?php echo 'Hello ' . $_POST["name"]; ?>
```

Sécuriser la plateforme (2/5)

Les serveurs...

- Système : SELinux, OSSEC, fail2ban
- Serveur web : suPHP, PHP-FPM, suhosin
- Applications web : ModSecurity, NAXSI

Sécuriser la plateforme (3/5)

Le réseau...

- Trafic autorisé depuis Internet
  - HTTP/HTTPS
  - Pas de SSH (encore moins de FTP)
- Trafic autorisé vers Internet
  - Rien par défaut (éviter les DDOS)
  - Autoriser au besoin (sites de mise à jour des applis)
  - Utiliser un proxy filtrant (log du trafic)

Sécuriser la plateforme (4/5)

Et les applications

- Interfaces d'admin : HTTPS sinon rien
  - /administrator /wp-admin /manage ...
  - ACL (accès depuis réseaux internes et VPN)
- ACL selon destination du site
  - Pas d'intranet ouvert sur internet
- Usage parcimonieux des greffons
  - Qualité du code très variable
  - Soucis de compatibilité avec les mises à jour des applis

Sécuriser la plateforme (5/5)

L'utilisateur

- Envoûté par les promesses du web 2.0+
- Parfois développeur
- Rarement expert en sécurité
- Souvent de bonne volonté

Mais surtout client de la plateforme

Stresser les serveurs

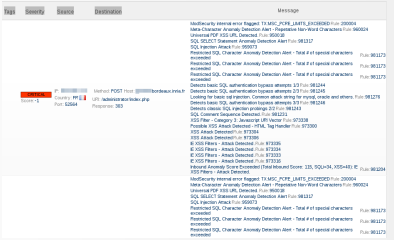
L'art de se faire peur

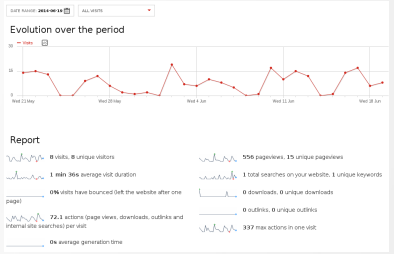
- Simplement
  - Apache Benchmark (ab)
- Brutalement
  - Siege
- Finement
  - Tsung, Funkload

Exploiter la plateforme (1/3)

Suivre l'activité quotidienne des serveurs

- Analyser régulièrement les logs...
  - Syslog, httpd, ModSecurity
- ...avec des outils confortables
  - Adiscon LogAnalyzer, AuditConsole
- Suivre l'évolution de la charge
  - Munin, Piwik





Exploiter la plateforme (2/3)

Appliquer les mises à jour...

...Toutes les mises à jour...

...du système ET des applis web

Exploiter la plateforme (3/3)

Sauvegarder

(et tester la restauration)

(Fichiers des sites/applis web, bases de données...)

Eat your own dog food

- Utiliser au quotidien les applications web déployées
  - Varier les manipulations
  - Essayer de pousser les applications dans leurs retranchements
- Sortir de l'environnement de son poste de travail pour entrer dans celui de ses utilisateurs
  - Couvrir différents environnements standards en mélangeant systèmes d'exploitation et navigateurs
- Avoir un regard critique sur la plateforme afin de la faire évoluer
  - Le web n'est pas figé

Se tenir informé

Toujours plus de veille

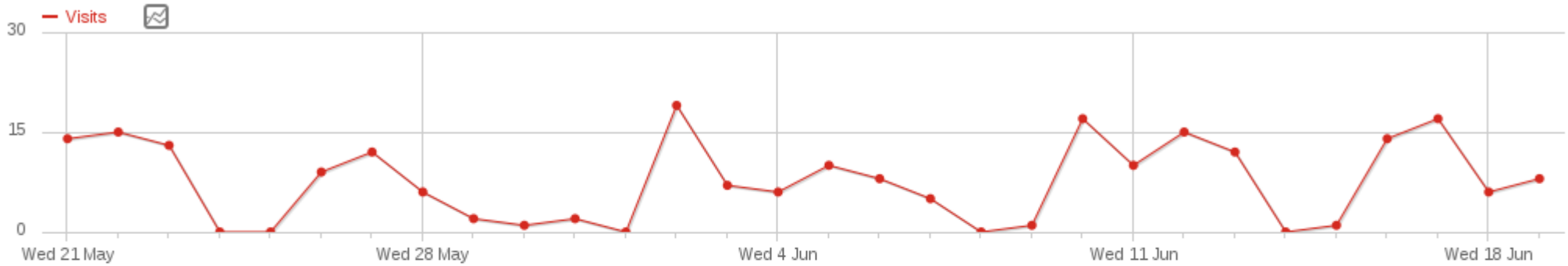
- Applications web
  - Indispensable : abonnement aux listes d'annonces
- CERT (-FR, Renater)
- Open Web Application Security Project -OWASP
- SANS/Internet Storm Center
- Observatoire de la Sécurité des Systèmes d'information et des Réseaux -OSSIR

Merci !

Tags	Severity	Source	Destination	Message
	CRITICAL Score:-1	IP: [redacted] Country: FR Port: 52564	Method: POST Host: [redacted]bordeaux.inria.fr URI: /administrator/index.php Response: 303	ModSecurity internal error flagged: TX:MSC_PCRE_LIMITS_EXCEEDED Rule:200004 Meta-Character Anomaly Detection Alert - Repetative Non-Word Characters Rule:960024 Universal PDF XSS URL Detected. Rule:950018 SQL SELECT Statement Anomaly Detection Alert Rule:981317 SQL Injection Attack Rule:959073 Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded Rule:981173 Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded Rule:981173 Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded Rule:981173 Detects basic SQL authentication bypass attempts 1/3 Rule:981244 Detects basic SQL authentication bypass attempts 2/3 Rule:981245 Looking for basic sql injection. Common attack string for mysql, oracle and others. Rule:981276 Detects basic SQL authentication bypass attempts 3/3 Rule:981246 Detects classic SQL injection probings 2/2 Rule:981243 SQL Comment Sequence Detected. Rule:981231 XSS Filter - Category 3: Javascript URI Vector Rule:973338 Possible XSS Attack Detected - HTML Tag Handler Rule:973300 XSS Attack Detected Rule:973304 XSS Attack Detected Rule:973306 IE XSS Filters - Attack Detected. Rule:973335 IE XSS Filters - Attack Detected. Rule:973334 IE XSS Filters - Attack Detected. Rule:973333 IE XSS Filters - Attack Detected. Rule:973316 Inbound Anomaly Score Exceeded (Total Inbound Score: 115, SQLi=34, XSS=40): IE XSS Filters - Attack Detected. Rule:981204
				ModSecurity internal error flagged: TX:MSC_PCRE_LIMITS_EXCEEDED Rule:200004 Meta-Character Anomaly Detection Alert - Repetative Non-Word Characters Rule:960024 Universal PDF XSS URL Detected. Rule:950018 SQL SELECT Statement Anomaly Detection Alert Rule:981317 SQL Injection Attack Rule:959073 Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded Rule:981173 Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded Rule:981173 Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded Rule:981173

DATE RANGE: **2014-06-19** ALL VISITS

Evolution over the period



Report

8 visits, **8** unique visitors

1 min 36s average visit duration

0% visits have bounced (left the website after one page)

72.1 actions (page views, downloads, outlinks and internal site searches) per visit

0s average generation time

556 pageviews, **15** unique pageviews

1 total searches on your website, **1** unique keywords

0 downloads, **0** unique downloads

0 outlinks, **0** unique outlinks

337 max actions in one visit