Ingénierie et Sécurité des Systèmes UNIX & Réseaux TCP/IP
10 ans d'expérience

Guillaume Arcas
Marié, 2 enfants
Né le 15 décembre 1968
Nationalité française
guillaume.arcas@free.fr

COMPÉTENCES TECHNIQUES

Systèmes d'exploitation (Installation & Administration)

- UNIX
  - Sun Solaris / IBM AIX
  - Linux Red Hat / GNU/Debian
  - FreeBSD 4.x / OpenBSD 3.x / Mac OS X 10.x
- Connaissance des environnements Microsoft Windows 95/98/NT/2000

Administration Réseaux TCP/IP

- Configuration de base (adressage IP, routage, etc.).
- Gestion des services Réseaux
  - DNS (BIND 8 et 9)
  - Serveurs de fichiers (NFS, SAMBA)
  - DHCP
  - Synchronisation temporelle (NTP)

Sécurité Réseaux

- Installation et configuration de pare-feux :
  - OS Linux : Netfilter/IPtables – ipchains - ipfwadm
  - OS *BSD : pf.
  - OS Sun Solaris : ipfilter
- Configuration de passerelles filtrantes à l'aide des outils système ;
- Installation de canaux chiffrés
  - ssh (OpenSSH), ssl (OpenSSL), stunnel, OpenVPN ;
- Analyse réseau : tcpdump, nmap (« scanner » TCP et UDP), Etherreal ;
- Audit de vulnérabilité : Nessus.
- Détection d'intrusion : Snort/ACID, Prelude-IDS, Honeyd.
- Journalisation : syslog, syslog-ng
- Supervision : NetSaint/Nagios, MRTG, RRDTool, Ntop.

Sécurité des Applications & des Données

- Sauvegarde
  - Time Navigator, Backup Express, Networker, Bacula
- Messagerie électronique
  - Sendmail, Postfix, Critical Path IMS (version 5 à 6)
- Solutions Antivirus SMTP/HTTP/FTP
  - TrendMicro VirusWall, Sophos, ClamAV
- Serveur Web : Apache, Zeus, IIS
- Serveur mandataire HTTP Squid 2.5
- Serveur FTP sécurisé ProFTPD.

- SGBD : MySQL, PostgreSQL, Oracle (notions d'administration)
- Haute disponibilité : LVS (Linux Virtual Server) & UltraMonkey

Langages de programmation

- PERL (Scripts CGI & Administration Systèmes / Réseaux)
- PHP (Développement d'interfaces SGBD/Web)
- Bash / Bourne Shell (Administration Systèmes / Réseaux)

Autres compétences

- Rédaction de documentation technique : Spécifications fonctionnelles et techniques, documentation Utilisateurs (Installation, Configuration, Administration, etc.), supports de cours
- Traduction technique anglais/français. Exemples : F.A.Q. OpenBSD, F.A.Q. IDS du SANS Institute, Guide de l'utilisateur PF (solution de filtrage IP pour OpenBSD).
- Rédaction de réponses à Appel d'Offres

Divers

- Interventions en tant que conférencier : Eurosec 2005, LSM2005, OSSIR, SSTIC 2005.
- Professeur vacataire auprès de l'EMIAE (Casablanca, Maroc) du groupe ESIAE.
- Co-fondateur de la branche francophone du projet SquirrelMail (www.squirrelmail-fr.org)
- Co-Fondateur du projet Retiaire (Sécurité Réseaux distribuée).
- Membre fondateur de la Team ZoZoA (Sécurité Réseaux IP et WiFi, Applications pratiques du Chiffrement)
- Membre actif de l'OSSIR (www.ossir.org).

LANGUES

- Anglais : courant.
- Allemand : lu, écrit et compris.
- Latin & Grec Ancien

PRINCIPALES MISSIONS DEPUIS 1994

INTEGRATEUR (ESSONNE)

Depuis juillet 2005
Direction des Services Professionnels

· Ingénieur Sécurité / DNS

Description de la mission

- Déploiement et sécurisation de serveurs DNS pour le compte d'un opérateur de téléphonie mobile.

Environnement technique

- Serveurs SUN Solaris
- Boitiers F5 3DNS
- BIND

PRESTATAIRE DE SERVICES DE GESTION DE NOMS DE DOMAINES (PARIS)

Juin 2005
Direction Technique

· Audit Sécurité

Description de la mission

- Evaluer le niveau de sécurité d'une plate forme d'hébergement de serveurs DNS et des services associés (site Internet, messagerie électronique)

Environnement technique

- Red Hat Linux
- BIND
- Serveurs Apache/Tomcat
- Bases de données MySQL

GROUPE CEGETEL SFR (BRANCHE MOBILE)

Sept. 2004 – mai 2005
Direction Technique des Services / Programme Sécurité

· Architecture et déploiement d'une solution de gestion centralisée des évènements de Sécurité

Description de la mission

- Mettre en place une solution de détection et de remontée des alertes de sécurité sur les plate-formes de services et d'interconnexion Mobile / Fixe
- Recenser et sélectionner les sources d'informations : flux réseau, journaux systèmes et applications, etc.
- Proposer une architecture modulaire, évolutive et sécurisée
- Développements des outils d'analyse et de présentation des rapports d'activité
- Mettre en production une maquette réduite pour évaluation

Environnement technique

- Red Hat Linux
- Suite Prelude-IDS
- Sondes Snort
- Bases de données MySQL & PostgreSQL
- Serveur Apache / PHP

GROUPE SFR CEGETEL / CEGETEL.RSS (TELECOMMUNICATIONS & INTERNET)

Février 2002 – Juillet 2004
Direction Technique – Ingénierie

· Mission d'ingénierie Systèmes & Réseaux pour le compte d'une entité de fourniture d'accès et de services Internet à des professionnels de Santé

Description de la mission

- Assurer la cohérence technique de la plate-forme de production, définir les plans et procédures des mises à jour logicielles (OS et applications).
- Accompagner la mise en oeuvre de nouveaux services tout au long du cycle de développement : choix des architectures, des technologies, des logiciels, rédaction des spécifications fonctionnelles et techniques, des guides d'installation, d'utilisation et d'administration, développements et accompagnement jusqu'à la mise en production.

Exemples

- Mise en place d'une solution de Webmail sécurisée (contrôle d'accès par carte)
- Mise en haute disponibilité de pare-feux
- Assurer le respect de la politique de sécurité Plate-Forme

- Tester unitairement les nouvelles versions des logiciels exploités ainsi que les nouveaux logiciels (Exemples : solutions antivirus Sophos, boitiers FortiGate)
- Support Niveau IV sur toute la plate-forme
- Veille technologique

Environnement technique

- Unix (Solaris majoritaire, Red Hat Linux).
- Messagerie (Critical Path IMS), Web (Apache), SGBD (Oracle 9i, MySQL 3.23).
- Pare-feux EADS M>Wall, Netfilter/IPtables
- Commutateurs Cisco Catalyst et Alteon.
- Serveurs antivirus (TrendMicro VirusWall)
- Scripts spécifiques en Shell (BASH; Korn-Shell), PERL et PHP.

Sécurisation des flux Internet HTTP

Description de la mission

- Assurer la sécurité des flux Internet grâce à une solution hautement disponible.
- Sécurité Réseau à l'aide de pare-feux redondants Netfilter/IPtables
- Sécurité Applicative (HTTP) à l'aide de serveurs mandataires (dont Squid) et du logiciel Antivirus InterScan VirusWall (version 3.8).
- Traitement transparent des flux HTTP non proxifiés (redirection dynamique des flux vers les serveurs Antivirus).

Environnement technique

- Red Hat Linux
- Solution de Haute Disponibilité et de Répartition de Charge LVS / UltraMonkey
- Serveurs antivirus (TrendMicro VirusWall)
- Serveurs mandataires HTTP (Squid)
- Scripts spécifiques en Shell (BASH; Korn-Shell), PERL et PHP.

Réponse à Appel d'Offres (GIE SESAM-Vitale)

Description de la mission

- Préconisation & choix de l'architecture (applicative & réseau) Cible
- Choix des technologies et des logiciels
- Définition de la politique de Sécurité
- Rédaction des demandes Fournisseurs et analyse technique des réponses
- Rédaction des spécifications techniques générales Plate-Forme

ANTERIA (SSII)

1997 - 2002
Direction Technique

Ingénieur d'études

Description de la mission

- Missions de courte durée (de quelques jours pour des audits à moins de 6 mois) pour des PME/PMI (majoritairement secteur de l'industrie) en France et en Europe
- Sauvegarde et Sécurité des Réseaux TCP/IP

Exemples de missions réalisées pour le compte de la SSII ANTERIA
Sauvegarde

- Installation de solutions de sauvegarde centralisée
- Assistance (support Niveau 2 et 3) et maintenance de solutions de sauvegarde Time Navigator

Sécurité

- Définition de la politique et de l'architecture de sécurité du site ;
- Identification et évaluation des risques ;
- Mise en adéquation plan de sécurité / risques identifiés ;
- Formation des équipes d'exploitation
- Audit réseau : utilisation de scanners (type nmap) et de logiciels ad hoc ;
- Installation des outils de protection (firewalls, passerelles filtrantes, antivirus) ;
- Simulation d'attaques (intrusion, déni de service, ingénierie sociale).

Environnement technique

- UNIX (Linux, Solaris, AIX), Windows 95/NT.
- Serveurs FTP, Web, messagerie, Samba.
- Firewalls ipfwadm et ipchains
- Outils nmap, Nessus (audit), Sniffit.

INTERLIANT EUROPE (SERVICES INTERNET EN MODE ASP)

Septembre 2000 – Septembre 2001
Direction Technique

Déploiement d'une solution de détection d'anomalies et de tentatives d'intrusion

Description de la mission

- Identifier et hiérarchiser le degré de vulnérabilité des différents serveurs et services ;
- Installation des outils d'audit (sondes Snort) ;
- Mise en place d'une base de journalisation centralisée (MySQL) ;
- Mise en place des interfaces d'interrogation (ACID et fonctionnalités spécifiques) ;
- Rédaction des procédures de maintenance et de mise à jour des signatures Snort ;
- Intégration aux outils de supervision réseau (NetSaint/Nagios et MRTG) ;
- Analyse de codes hostiles et analyse après attaques (réelles ou supposées).

Environnement technique

- Unix (Linux majoritaire, Solaris), Windows 2000 Advanced Server.
- Serveurs FTP, Web (Apache, Zeus), messagerie, serveurs de fichiers NFS et Samba.
- Réseau majoritairement switché (Cisco Catalyst) et à répartition de charge (Alteon).
- Outils nmap, snort, ACID.
- Développement de fonctionnalités spécifiques en PERL et PHP.

Déploiement et administration d'une plate-forme d'hébergement Internet (serveurs dédiés et mutualisés).

Description de la mission

- Réception des documents Plate-Forme (Guides d'installation)
- Montage de la plate-forme
- Installation des serveurs (OS et applications)
- Mise en place des scripts d'administration et d'activation de comptes (les services étant activables 24h/24 après prise de commandes en ligne)
- Maintenance du site de commerce électronique permettant la commande de services (ColdFusion et serveur Oracle)

Environnement technique

- Unix (Linux majoritaire, Solaris), Windows 2000 Advanced Server.
- Serveurs DNS (BIND), FTP, Web (Apache, Zeus), messagerie (Dmail), serveurs de fichiers NFS et Samba, SGBD (MySQL).

FILIALE INTERNET D'UN GROUPE AUTOMOBILE

Mai – août 2000

Sécurité de sites Web

Description de la mission

- Définition de la politique de sécurité du site ;
- Choix des technologies ;
- Sécurisation du système d'exploitation et des serveurs (Apache, IIS) ;
- Suivi d'activité.

Environnement technique

- Serveurs Apache sur Linux et IIS sur Windows NT ;
- Serveurs de Bases de données (Oracle 8i, PostgreSQL, MySQL).

GROUPE FAURECIA (EQUIPEMENTIER AUTOMOBILE)

Interventions de courtes durées
France & Allemagne

Assistance à l'administration de la solution de sauvegarde centralisée

Description de la mission

- Définition des procédures (types de sauvegarde, fréquences, gestion des bandes ...) ;
- Installation des logiciels de sauvegarde (Time Navigator) ;
- Formation des équipes d'exploitation ;
- Suivi d'exploitation.

Environnement technique

- UNIX (HP-UX, AIX, Solaris), NT, Windows 95, Novell.
- Logiciel de sauvegarde Time Navigator (Quadratec).
- Librairies de bandes magnétiques Tandberg, Exabyte, Overland.

CABINET INFO SECTORIS (ETUDES MARKETING)

1994 - 1995

· Veille technologique et marketing sur la Sécurité Internet & Réseaux TCP/IP

Description de la mission

- Etat de l'art ;
- Choix des sources d'information, gestion des abonnements aux listes de diffusion ;
- Mise en place d'une structure d'alerte ;
- Comptes rendus de conférences spécialisées (InfoWarCon Europe...).

FORMATION

1993 : DUT «Marketing et Techniques de Commercialisation» (IUT Sceaux) / Informatique (auditeur libre, Paris XI Orsay)

1992 : DEUG Droit (auditeur libre, Université Paris XI Sceaux).
1990 : Bac série B (Sciences Economiques & Sociales).
1986 : Bac série A1 (Lettres & Mathématiques)

DIVERS

Titulaire du permis B. Mobilité sur Paris et IDF, possibilité de missions de courte durée en province et à l'étranger
Sports pratiqués : natation, tir sportif (carabine et pistolet Plomb 10 mètres), plongée libre et bouteille (Niveau II).
1990 : Service Militaire Actif (Armée de l'Air)