

Philippe Bourcier

53, rue Truffaut
75017 Paris

E-mail : philippe@cyberabuse.org
URL : <http://www.cyberabuse.org/philippe/>
Tel : +33 6 63 85 32 32
Date de naissance : 04/06/80

ARCHITECTE EN SECURITE, SYSTEMES ET RESEAUX

Expérience Professionnelle

15/01/2008 – en poste CRITEO **Senior IT Engineer**
Architecte infrastructure haute-disponibilité, Ingénierie réseau BGP, Load-Balancing, monitoring, bases de données, automatisation, intégration et développements logiciels libres et solutions dédiées.

06/01/2003 – 12/01/2008 CITALI **Consultant SSI**
Chef de projet SSI (sécurisation, évolution d'architectures...), Architecte infrastructure grand compte (services réseau, services Internet, sécurité, clusters, haute dispo...), troubleshooting LAN/WAN, audits techniques sécurité, tests d'intrusion, intégration et développements logiciels libres et solutions dédiées (radius/netflow/active directory/webdav...), veille technologique.

01/03/2002 – 30/06/2002 GIP RENATER **Stage CERT-RENATER**
Analyse de compromissions, gestion d'incidents de sécurités (attaques DDoS, compromissions, ...), veille technologique, développement intranet et extranet, mise en place du serveur DNS IPv6 pour la zone .FR, honeypots, mise en place d'un labo de test des codes hostiles...

01/03/2001 – 30/09/2001 XP CONSEIL **Consultant Junior SSI**
Politique de sécurité, audit politique anti-virus, audit sécurité Windows 2000, développements intranet, mise en place du labo de test...

Expérience Personnelle

Depuis juin 2002 FRNOG www.frnog.org
Animateur/Organisateur
Forum de discussion français des experts techniques réseaux et sécurité des réseaux. Organisation de conférences sur la sécurité et les réseaux opérateurs, hébergeurs et autres acteurs d'Internet.

Depuis mai 2002 NETLANTIS www.netlantis.org
Chercheur/Développeur
Projet de recherche, analyse et représentation graphique (cyber-géographie) du routage internet (BGP).

Depuis juillet 2000 CYBERABUSE www.cyberabuse.org
Chef de projet/Développeur
Gestion des projets, conférences, publications, développements d'outils et logiciels GPL (PHP/SH/C++/SQL), serveur whois.cyberabuse.org, administration de serveurs unix et bases de données...

Depuis juin 2000 UNDERNET www.undernet.org
Administrateur
Administrateur de plusieurs serveurs IRC dont :
- proxyscan.undernet.org : premier scanner de proxy vulnérables sur IRC
- Bucharest.ro.eu.undernet.org : serveur conçu pour résister aux attaques DDoS

Formation	<p>1998 – 2002 Institut International du Multimédia (www.devinci.fr/iim) Formation en 4 ans au métier de chef de projet multimédia : - 2 années de cours techniques sur les NTIC - 2 années de cours théoriques sur le management et la communication</p> <p>1998 Bac S spé. Physique-Chimie au Lycée Privé St Joseph (Vendée)</p>
Compétences Techniques	<p>OS : Linux (debian/redhat/centos), Free/Open/Net BSD, Solaris, Windows, MacOS, Cisco IOS, Linux embarqués, *nix...</p> <p>DB : MS SQL 2005, MySQL 5.x, Memcached</p> <p>Web : Apache, Nginx, Lighttpd, WebDAV, mod_proxy, mod_memcache...</p> <p>Sécurité, Services IP : 802.1x, FW-1, Cisco ASA, mod_security, Snort, OpenVPN, OpenSSL, ipfilter, ipfw, VPNs (IPSEC/SSL), DNS, DHCP, Radius, VoIP...</p> <p>L2-L3 : BGP, STP, HSRP...</p> <p>Langages : PHP, SH, SQL, HTML, C/C++, CGI, Perl...</p> <p>Divers : Office, OpenOffice, Project, Photoshop...</p>
Contributions Open-Source	<p>Cameleon : C++/SH/PHP – système de filtrage de la publicité sur les pages web</p> <p>NFSen : contribution à l'interface graphique du logiciel de statistiques NetFlow</p> <p>Zcw : C++/SH/sqlite – solution de recherche de contact abuse</p> <p>gala : PHP – analyse géographique des sources d'attaques dans les logs</p> <p>mod_security : contribution aux règles de filtrage proposées par défaut</p> <p>scponly : C – port Win32</p> <p>Radalyser : C++/PHP – interface graphique d'analyse de logs radius accounting</p> <p>Proxywifi : PHP/SH – HotSpot avec fake dns et authentification</p>
Conférences et Publications	<p>Eurosec 2000, Paris – Le projet Cyberabuse</p> <p>ZDNet, Octobre 2000 – Interview "Experts warn of multiple computer attacks"</p> <p>FIRST 2001, Toulouse – The CyberAbuse project</p> <p>FIRST 2002, Honolulu – The CyberAbuse project [annulée]</p> <p>Réunion OSSIR 2003, Paris – L'attaque des clones</p> <p>JSSI du Celar 2003, Bruz – Protection des infrastructures Internet, la piste BGP</p> <p>RIPE-46, Amsterdam – Realtime Analysis of BGP Routing Tables</p> <p>Eurosec 2004, Paris – Poste de travail : Le maillon faible</p> <p>JSSI du Celar 2006, Bruz – Démonstration d'interception (écoute) VoIP</p> <p>Les Echos, 12 Février 2006 – Interview sur la sécurité de la VoIP</p> <p>Eurosec 2007, Paris – Virtualisation et DNS IDS</p> <p>Depuis 2002, FRnOG – Organisation et comité de programme</p>
Langues Vivantes	<p>Français : langue maternelle</p> <p>Anglais : bilingue</p>
Centres d'intérêt	<p>Loisirs : informatique, promenades, cinéma, VJing, voyages</p> <p>Culture : musique et arts psychédéliques, arts contemporains</p> <p>Sport : VTT, bodyboard, surf</p>