VECTEN Sébastien
Consultant Sécurité, 38 ans
Nationalité Française
Permis B, Véhicule

Web : www.insecurity.fr
Mail : info@insecurity.fr
Pgp : 0x2A4FD1A4D1364A97

Consultant Sécurité Sénior / Pentester Freelance
15 ans d'expérience

COMPÉTENCES

Compétences techniques	Tests d'intrusion : Interne/Externe, Infrastructure, Applications Web, Clients lourds, Bases de données, Web Services/API, Wifi, VOIP... Audits de sécurité : Audits d'architecture, relevés et analyses de configurations, audits de code, audits techniques SOX, HDS et PCI-DSS. Reverse Proxy / Load Balancing : F5 BigIP (LTM, ASM, APM). IDS/IPS : Snort, Fortinet. Firewall : Checkpoint, Fortinet, Iptables, Netscreen, Cisco Pix. Systèmes : Connaissances avancées des OS Windows Serveur et Unix/Linux. Développement : Python, Java/J2EE, C/C++, Perl, PHP et Bash
Compétences personnelles	Forte adaptation au changement de contexte, Rigueur, autonomie et travail en équipe, Gestion de projet et direction de missions en sécurité, Bonnes qualités rédactionnelles (plus de 350 rapports rédigés), Sens de l'écoute et aisance à l'oral, Intégrité, éthique et respect de la confidentialité.
Compétences linguistiques	Français : Langue maternelle. Anglais (Écrit) : Niveau intermédiaire. Anglais (Oral) : Connaissances professionnelles.
Clients	ADEO, ADP, AG2R, Ariane Espace, Auchan, AXA(FR), AXA(BE), AXA TECH, Bizz Dev(BE), Blitz, Boulanger, Bouygues Telecom, BRED, CACF, CACP, CAIMMO, Canon, CAPH, CASA, Casino, CDC, Cegid, CH Oyonnax, Chevreux, Contentia, Crédit Coopératif, CTIE(LU), Digitick, FFF, FGDR, Galderma, Gaselys, Gemalto, GEODIS Calberson, Groupama, HCL, Interpol, ITCE, Kewego, Kiabi, Labio, Lafarge, Leroy Merlin, M6, MAIF, Manpower, Mondadori, Monecam, Natixis, Nexity, NextiraOne, NRB, Parel(SG), PMU, Rothschild, Samse, Sanofi, SGCIB, SITA, SMABTP, SNCF, Société Générale, Softway Medical, Somfy, Suez, TF1, Total, UEM, Veolia, Verspieren, VSE, Wafasalaf, etc.

EXPERIENCE PROFESSIONNELLE

INSECURITY — France
Société spécialisée en sécurité offensive — 1 collaborateur
FONDATEUR ET GÉRANT / PENTESTER FREELANCE — Depuis Juin 2016

Réalisation de tests d'intrusion et d'audits techniques. Participation à de nombreux programmes de Bug Bounty privés.

LEXSI / XS POLE SECURITE — Lyon / Lille - France (69/59)
Société de conseil spécialisée en sécurité informatique — 200 collaborateurs
CONSULTANT SÉCURITÉ SÉNIOR / PENTESTER — Mai 2013 à Février 2016

J'ai réalisé au sein de cette société plus d'une centaine d'audits de sécurité et tests d'intrusion complexes pour des grands comptes appartenant au secteur bancaire, grande distribution, défense, assurance, immobilier et santé. Voici quelques exemples de missions qui m'ont été confiées :

- Tests d'intrusion / audits réseau ou applicatifs internes, externes, en boite noire, grise et blanche,
- Audits d'architecture, tests de cloisonnement, scans de vulnérabilité, relevé de configuration...
- Développement d'outils (python), gestion de projet, direction de mission et avant-vente.

VECTEN Sébastien
Consultant Sécurité, 38 ans
Nationalité Française
Permis B, Véhicule

Web : www.insecurity.fr
Mail : info@insecurity.fr
Pgp : 0x2A4FD1A4D1364A97

MGSMEDICAL — Saint-Dizier - France (52)
Société d'édition logicielle - Secteur SANTÉ — 3 collaborateurs
CRÉATEUR D'ENTREPRISE ET GÉRANT — Octobre 2011 à Janvier 2013

Création et gestion d'une SARL dont le but est le développement et la commercialisation d'un logiciel complet de gestion de cabinet médical à destination des dentistes.

- Gestion de projet, Analyse (Merise / UML), administration et développement d'application (Java Swing/SwingX/JGoodies). Interaction avec les APIs bas niveau SESAM Vitale.

PROVADYS / CHECKMATES — Boulogne Bill - France (92)
Société de conseil – Secteur Sécurité SI / Finance — 25 collaborateurs
CONSULTANT SÉCURITÉ CONFIRMÉ / PENTESTER — Nov 2010 à Juin 2011

J'ai réalisé au sein de cette société de multiples audits de sécurité et tests d'intrusion complexes pour des grands comptes appartenant au secteur bancaire, grande distribution, pharmaceutique, aéronautique et assurance. Voici quelques exemples de missions qui m'ont été confiées :

- Tests d'intrusion / Contre audits applicatifs internes, externes, en boite noire ou boite blanche.
- Série d'audits techniques sur un périmètre monétique national dans le cadre de la norme PCI-DSS.
- Scan de ports, de vulnérabilités, puis tests d'intrusion sélectifs sur le périmètre Internet externe d'un grand groupe à l'échelle mondiale (environ 8000 IP au départ).

BRITISH TELECOM — Paris 13ème - France (75)
Société de services – Secteur Réseau / Télécom — 2600 collaborateurs en France
CONSULTANT SÉCURITÉ / INTÉGRATION & ARCHITECTURE — Janvier 2010 à Nov 2010

Ingénierie, design d'architecture et intégration de solutions de sécurité, pour des institutions publiques (ministère du Travail et de l'Éducation) et plusieurs groupes du secteur privé (Télécom, Santé et Énergie).

Pour chaque mission, une étude de l'existant et des impacts niveau 1 à 7 sur des problématiques d'accès, de supervision, de sauvegarde, de mise à jour, de segmentation réseau et de dimensionnement ont été observées.

Voici quelques exemples de missions qui m'ont été confiées :

- Design & Intégration d'une solution de reverse proxy F5 afin de sécuriser et Load Balancer l'ensemble des applications Internet critiques (environ 20) du groupe.
- Changement en production d'une double couche de firewall (cluster ASA & Netasq par un cluster Checkpoint & Fortinet) et ajout de fonctionnalités IPS (Fortinet).
- Réalisation de maquettes complexes pour des démonstrations d'avant-vente (Antispam CISCO IronPort, Antivirus / Antispam Trend Micro, Juniper Steel Belt Radius), Upgrade de firewall (Checkpoint), rédaction de procédures, installation de serveurs, etc.

Technologies rencontrées : F5 BigIP (LTM, ASM, APM), Checkpoint, Fortinet (Firewall, IDS/IPS), Juniper Netscreen (Firewall), Cisco (Switching).

CYBER NETWORKS (RACHETÉ PAR BRITISH TELECOM) — La défense - France (92)
Société de conseil spécialisée en sécurité informatique — 180 collaborateurs
CONSULTANT SÉCURITÉ / PENTESTER — Octobre 2007 à Janvier 2010

Réalisation de nombreux audits de sécurité et tests d'intrusion pour des grands comptes des secteurs Banque, Assurance, E-commerce, Énergie, Transport, Télécom, Grande Distribution, Sport, Santé et Intérim.

- Réalisation d'une campagne de tests d'intrusion interne sur une vingtaine d'applications bancaires critiques (Trading, Ressources Humaines, Administration distante, Gestion des prestataires).
- Tests d'intrusion, contre audits, audits de code internes et externes en boite noire et boite blanche :
  - Banques en ligne pour particuliers, Billetterie en ligne, Portails d'assurance,
  - Portails d'investissements boursiers en ligne, Portails RH, de congés, de paye/compta,
  - Solutions de réservation de voyages, de gestion des prestataires, Plateforme WebSSO, etc.
- Tests du stagiaire et social engineering (Physique, Campagne de phishing, chevaux de troie, etc.).
- Cartographie wifi et recherche de bornes frauduleuses.
- Scans de vulnérabilités ponctuels et récurrents (Nessus, Qualys, Criston).
- Relevés et audits de configuration divers (Checklists personnelles, Sans et CISecurity) :

VECTEN Sébastien
Consultant Sécurité, 38 ans
Nationalité Française
Permis B, Véhicule

Web : www.insecurity.fr
Mail : info@insecurity.fr
Pgp : 0x2A4FD1A4D1364A97

- Sur des systèmes d'exploitation : Windows Serveur et AD, Linux Red Hat, Solaris,
- Sur des bases de données : Oracle, MSSQL et MySQL,
- Sur un serveur d'application Tomcat et sur des équipements de type Firewall (Checkpoint, Pix).

ARESSI — Reims - France (51)
Éditeur de solutions de sécurité — 10 collaborateurs
STAGIAIRE INGÉNIEUR SÉCURITÉ - NIVEAU MASTER2 — Avril à Septembre 2007

L'objet de mon stage de master 2 a été d'étudier et d'implémenter la sécurisation de la Voix sur IP niveau Firewall / IDS au sein d'une Appliance de sécurité tout en respectant la qualité de service.

- Étude de l'état de l'art en matière de sécurisation Voix sur IP, étude des protocoles et tests d'attaques,
- Intégration d'un préprocesseur SIP pour Snort (IDS) et édition de signatures,
- Validations, tests de montée en charge, et génération de trafic afin d'analyser l'impact sur la QOS.

Mots clés : IDS/IPS Snort, Firewall Iptables, SIP, QOS Diffserv, H323, IAX, RTP, Man In The Middle

ARESSI — Reims - France (51)
Éditeur de solutions de sécurité — 10 collaborateurs
STAGIAIRE INGÉNIEUR SÉCURITÉ – NIVEAU MASTER1 — Mai à Juillet 2006

Optimisation des sondes de détection/prévention d'intrusions réseau d'une Appliance de sécurité en vue de réduire le nombre de faux positifs générés en dessous de 5%.

- Optimisation dynamique de la configuration et les règles de l'IDS selon la configuration du pare-feu.
- Développement d'interface Web (CGI Perl) de gestion des signatures et du fichier de configuration des sondes.
- Développement et Intégration d'un robot de mises à jour automatiques et d'un parseur de signatures Snort.

Mots clés : IDS/IPS Snort, Firewall Iptables, Développement C, Bash et CGI Perl.

INTERVENTIONS DIVERSES

2020 : Université de Reims Champagne-Ardenne - Intervenant extérieur en Master2 ASR

- Conférence professionnelle (CM) sur la présentation du métier de pentester,
- Rappels techniques et TP sur les différentes méthodes d'élévation de privilège sous Linux.

FORMATION & INFORMATIONS COMPLÉMENTAIRES

Diplômes	**2007** : Master Professionnel Administration et Sécurité des Réseaux - Mention AB - Université de Reims Champagne-Ardenne. **2005 :** Licence Informatique - Mention Assez Bien (AB) - Université de Reims (URCA). **2004** : Brevet de Technicien Supérieur en Administration des Réseaux Locaux d'Entreprise - Lycée Marie Curie – Marseille.
Formations	**2010 :** Formation et certification F5 LTM Advanced - *ID SEL 3847* - Westcon Security. **2010 :** Formation et certification F5 LTM Essential - *ID PCL 5532* - Westcon Security. **2010 :** Formation F5 modules ASM & APM - Westcon Security / F5. **2010 :** Formations internes (2 jours) Checkpoint (SPLAT) et BlueCoat - Bristish Telecom. **2009 :** Formation et Certification EC-Council CHFI - *ID ECC934135* - Computer Hacking Forensic Investigator. **2009** : Formation et Certification QualysGuard - Qualys. **2008** : Formation CYBER-NETWORKS Développement d'Applications Web Sécurisées. **2007** : Formations NET2S finance (Fonctionnel Finance, Asset Management).
Centres d'intérêt	Informatique (Sécurité et Intrusion), Guitare et Sports de combat (pratique du Full-Contact pendant 10 ans et jiu-jitsu pratiqué pendant 2 ans), Musculation…