Alexis BRAZ NOGUEIRA
93, Rue Victor Hugo
92800 Puteaux
alexis@bnogueira.com
06 46 66 36 27
33 ans
Permis A & B

Consultant Sécurité

DIPLÔMES

2012 : Ingénieur Informatique option Systèmes, Réseaux et Télécom – INGESUP, Paris

2009 : Prépa Math SPE ATS – Adaptation de Technicien Supérieur – Lycée Diderot, Paris

2008 : BTS Conception et Industrialisation en Microtechniques – Lycée Jules Richard, Paris

2006 : BAC STI – Génie Mécanique – Paris

COMPÉTENCES INFORMATIQUES

Langages : HTML/CSS, PHP/MySQL, JavaScript, Scripting Shell, PowerShell, Batch, Python, Golang, VBA

Systèmes Windows : XP, 7, Server 2003, Server 2008, Server 2012, Server 2016

Systèmes Unix : Linux (Redhat, Debian, Gentoo), FreeBSD

Systèmes Divers : ESX, Hyper-V, AS400, Citrix, Lotus Domino, Cloud Azure

Serveurs Web : Nginx, Apache Webserver, Apache Tomcat, JBoss, Microsoft IIS, Golang

Base de données : MySQL, MS-SQL, Oracle, PostgreSQL, Sybase, AS400

Softwares: BurpSuite, Sqlmap, Metasploit, JohnTheRipper, Mimikatz, SysInternals, WinDbg, OpenVAS, Nmap, Wireshark, Aircrack, Snort, Ossec, Scapy, Qualys, Nessus, PowerBi

DOMAINE DE COMPÉTENCES

Tests d'intrusion : externe et interne, client lourd, infrastructure Microsoft & Unix, Wi-Fi, cloisonnement réseau, VoIP/ToIP, AS400, application mobile (Android/iOS), RedTeam

Relation Client : Gestion des prestataires à l'international, Identification du besoin

Encadrement : Management d'une équipe de 4 personnes, Formation de consultants juniors

Maitrise opérationnelle : Administration système, réseaux, sécurité et sauvegarde

COMPÉTENCES LINGUISTIQUES

Anglais : Courant
Espagnol & Portugais : Compréhension orale

LOISIRS

Hobbies *: Running et Voyages*
Adepte de challenges informatiques

EXPERIENCES PROFESSIONNELLES

FEVRIER 2019-2021 – CONSULTANT SECURITE – AXA FRANCE

Missions : *Assurer le bon déroulement de la plateforme pentest*

⇒ Réalisation et suivi des audits de sécurité (Pentests et ACPR)
⇒ Rejeux de vulnérabilités à la suite de la mise en place de correctifs (Kali)
⇒ Création d'un site web d'historisation des pentests (Golang/SQLite)
⇒ Mise en place de KPI (PowerBI)
⇒ Formation de sensibilisation vis-à-vis des DEV et des nouveaux entrants
⇒ Développement d'une solution interne pour la gestion des pentests (VBA)
⇒ Mise en place des recommandations du groupe sur la partie pentest
⇒ Participation aux incidents de sécurité et contrôles sous-traitants
⇒ Sécurisation du cloud avec Azure Sentinel
⇒ Suivi des filiales et des RSSI dans la gestion des vulnérabilités
⇒ Suivi budgétaire et des relations avec les partenaires pentest
⇒ Management de 4 personnes

JUIN 2016-2019 – ADJOINT RSSI – GENERAL ELECTRIC MONEY BANK

Missions : *Accompagner le RSSI sur les parties techniques*

⇒ Mise en place d'un SOC
⇒ Analyse et cartographie des risques
⇒ Communication sécurité (Incidents, SOC, Sensibilisation)
⇒ Suivi des audits de sécurité (Pentests et SOx)
⇒ Aide au choix de solutions techniques de sécurité (IAM, DLP, AV, CASB)
⇒ Reporting et comité sécurité en Anglais
⇒ Implémentation des politiques de sécurité GE

SEPTEMBRE 2012-2016 – CONSULTANT SECURITE - LEXSI

Missions : *Réalisation de missions de pentest en France*

⇒ Plus de 90 missions en Tests d'Intrusion (Interne et Externe)
⇒ Evaluation des risques, des Menaces et des Conséquences
⇒ Sensibilisation, Préconisation et Recommandation
⇒ Rédaction de rapports en Français et en Anglais
⇒ Restitution managériale et technique
⇒ Avant-vente technique
⇒ Conduite de projets et gestion du planning
⇒ Encadrement de consultants juniors
⇒ Rédaction de guide (avant-vente, check-list auditeur)
⇒ Responsable des machines d'attaques et du Wiki Interne sous Gentoo

SEPTEMBRE 2010-2012 - CONSULTANT - ALTRAN CHEZ GDFSUEZ

Missions : Assurer le maintien d'une plate-forme de services liés au cycle de vie des logiciels de la Direction de la Recherche et de l'Innovation.

⇒ Gestion des versions logicielles (Subversion)
⇒ Gestion du workflow des projets liés aux logiciels (Mantis Bug Tracker)
⇒ Automatisation de la génération de devis et PV de livraison (PHP/MySQL)
⇒ Optimisation des tâches répétitives (Powershell)
⇒ Mise en place d'outil de supervision (EyesOfNetwork)
⇒ Mise en place d'un reverse proxy (Nginx/Apache)
⇒ Animation des Comités de Pilotage
⇒ Conduite de projets

Exemples de missions

Ingénieur Qualité Logicielle - 2009

Au cours de l'année passée chez SkyRecon, j'ai été amené à contrôler le logiciel HIPS créé par l'éditeur. Les tests portaient à la fois sur le système Windows que sur la couche réseau (Overflow, Rootkit, Cryptologie, Keylogger, Registry, Firewall, DDoS)

Pour des raisons automatisation d'images systèmes, j'ai développé des scripts Bourne Shell et pour de l'optimisation des plans de tests d'autres scripts en Powershell.

Tests d'étanchéité et de cloisonnement réseau

Cette mission avait pour but de tester le niveau de sécurité du SI et de vérifier le cloisonnement réseau entre TF1 et SODEXO. L'audit portait principalement sur la segmentation des différents VLAN (Monétique, Datacenter,...) et aussi sur l'efficacité des équipements de filtrage afin de déterminer la possibilité pour un individu d'atteindre des zones sans en avoir les autorisations.

Audit de sécurité du SI

Tests d'intrusion du SI siège ainsi que de l'ensemble des SI des sites interconnectés situés dans différent pays. L'audit avait notamment pour objectif d'énumérer les vulnérabilités permettant à un utilisateur de compromettre le domaine Active Directory des différents sites et de démontrer les différentes possibilités d'exfiltration de données.

Tests d'intrusion applicatifs

Multiples tests de d'intrusion sur de nombreuses et diverses applications du monde bancaire.

Les tests avaient pour objectifs d'éprouver la sécurité d'applications web ou de clients lourds s'appuyant sur différentes technologies (Citrix,..). Outre les tests classiques sur des vulnérabilités exploitables par injection de code (XSS, SQLi, CSRF, etc..), une analyse du comportement de l'application amenant, par exemple, des tests spécifiques d'étanchéité des sessions, d'analyse des flux réseaux ou de détournement des fonctionnalités ont été systématiquement réalisés.

Tests d'application avec authentification forte

Audit d'un portail de l'État du Luxembourg destiné à permettre l'accès à l'ensemble des démarches administratives des citoyens et des professionnels. L'application mettant en œuvre de l'authentification forte par carte à puce.

Tests d'intrusion externe et interne

Mission de test d'intrusion externe et interne dans le contexte du « stagiaire malveillant ».

Les tests avait pour but d'éprouver la sécurité du SI avec une approche uniquement en mode boite noire. Dans une première phase en faisant un test externe afin de tenter d'atteindre l'intérieur du SI et dans une seconde phase un test d'intrusion interne, avec authentification 802.1x, à partir d'un poste utilisateur en ayant pour objectifs de récupérer des documents confidentiels.

Audit de configuration Windows

L'analyse de la sécurité du système Windows avait pour but de vérifier une multitude de points de contrôle.

Ces points de contrôle devaient mettre en évidence des défauts de configuration systèmes (Sécurité des comptes, Sécurité des journaux, Sécurité des services, Patch Management, …) et réseaux (Niveau d'authentification, Pare-feu, Session utilisateur, …).

Audit d'un poste nomade

L'audit avait pour objectif de s'assurer du bon durcissement de la sécurité du poste nomade Windows mais aussi de simuler un attaquant malveillant connecté en VPN.

Tests d'intrusion Wi-Fi

Cette mission avait pour but de tester la sécurité d'un point d'accès Wi-Fi en utilisant les vecteurs d'attaques propres à cette technologie (interception des flux, cassage ou réutilisation de clé de chiffrement, mise en place de faux points d'accès, robustesse des certificats) afin d'obtenir un accès illégitime à des ressource du SI interne.

Audits applicatifs client-serveur

Multiples audits de plateformes applicatives avec des architectures 2 tiers et 3 tiers.

Les tests d'intrusion portaient sur des applications de type client lourd alliant différentes technologies (VBA, PowerBuilder, C, JAVA, …) mais aussi des applications Web développés dans divers langages (ASP, PHP, Applet Java, …).

Audit de la robustesse des mots de passe

Analyse de la robustesse des mots de passes des utilisateurs de plusieurs domaines à partir de la base des comptes. Les statistiques ont été réalisées grâce à la plateforme de cassage de mot de passe LEXSI.

Scans de vulnérabilités

Missions d'audit de scans de vulnérabilités afin d'identifier les vulnérabilités les plus importantes dans de courts délais.

Tests d'intrusion en conditions réelles (RedTeam)

Missions de tests d'intrusion en conditions réelles. L'objectif étant, à partir d'internet, de déterminer jusqu'où un attaquant serait en mesure de pénétrer au sein du système d'information. Un point d'attention particulier étant apporté à la discrétion.

Audit de Web Services

Audits d'une plateforme de service incluant des Web Services relatifs au développement d'une nouvelle méthode de paiement bancaire via un prestataire de service de paiement (PSP).

Tests d'intrusion interne et VoIP/ToIP

L'objectif premier était d'éprouver la sécurité du SI avec une approche en mode boite noire. Et dans un second temps d'effectuer des tests d'intrusion sur l'infrastructure ToIP (Méthode d'authentification, écoute de communications, injection de flux RTP,…).

Pilotage de l'activité Pentest

Au sein d'AXA France, j'ai été amené à réaliser des tests d'intrusion mais aussi des rejeux à la suite d'un test d'intrusion qui aurait pu être réalisé par un prestataire.

Au bout d'un an j'ai repris le pilotage du pôle pentest avec 4 personnes à manager.